UNIVERSITE D'AIX-MARSEILLE

ED 372 SCIENCES ECONOMIQUES ET DE GESTION

IAE d'Aix-en-Provence

CERGAM / EA 4225

Thèse présentée pour obtenir le grade universitaire de docteur

Discipline : Sciences de Gestion, Section CNU n°6

Benoît FANTINO

Quels éléments d'influence pour l'adoption symbolique de la sécurité des systèmes d'information ?

Soutenue le 17 décembre 2018 devant le jury :

Rapporteurs :	**Sabine Carton** Professeur des Universités en Sciences de Gestion, CERAG (FRE 3748), Grenoble IAE, Université Grenoble Alpes
	Claire Gauzente Professeur des Universités en Sciences de Gestion, LEMNA (EA 4272), Université de Nantes
Suffragants :	**Cécile Godé**, Professeur des Universités en Sciences de Gestion, CRET-LOG (EA 881), Faculté d'Économie et de Gestion, Aix Marseille Université
	Claudio Vitari Professeur des Universités en Sciences de Gestion, CERGAM (EA 4225), Faculté d'Économie et de Gestion, Aix Marseille Université
	Emmanuel Houzé Maître de Conférences, Habilité à diriger les recherches, MRM (EA 4557), IAE de Montpellier, Université de Montpellier II
Directeur de la Recherche :	**Serge Amabile** Professeur des Universités en Sciences de Gestion, CERGAM (EA 4225), Faculté d'Économie et de Gestion, Aix Marseille Université

« L'Université Aix-Marseille n'entend donner aucune approbation ni improbation aux opinions émises dans les thèses ; ces opinions doivent être considérées comme propres à leurs auteurs. »

À Leslie, À Loup, À Choupette…

Résumé

La sécurité des systèmes d'information (SSI) est une discipline jeune dont l'intérêt s'inscrit dans la dépendance croissante des entreprises envers leur SI et en perspective du nombre grandissant d'incidents de sécurité. Dans cette recherche, nous nous intéressons à la gestion des risques SI, pour laquelle la littérature souligne le manque d'implication des top-managers.

Nous abordons cette problématique sous l'angle de la décision des dirigeants pour la SSI, au travers de quatre approches théoriques : les modèles des perceptions managériales des risques SI (Goodhue et Straub 1991 ; Straub et Welke 1998), la perception des risques en psychologie (Douglas et Wildavsky 1983 ; Fischoff et al., 1978 ; Sjöberg et al. 2004 ; Slovic et al. 1979 ; Wildavsky et Dake 1990 ; Yates et Stone 1992), la théorie néo-institutionnelle (Di Maggio et Powell 1983 ; Scott 2005) et la théorie sur l'adoption symbolique des innovations (Karahanna et al. 1999 ; Karahanna et Agarwal 2006 ; Klonglan et Coward 1970).

L'objectif de nos travaux est de rendre intelligible les influences sur l'adoption symbolique de la SSI. Après avoir adapté le modèle d'adoption symbolique à la SSI, nous employons une méthode qualitative organisée autour de 17 études de cas dans des entreprises d'activités variées. La SSI y est alors observée comme un processus de décision de gestion des risques SI. Nos résultats montrent la pertinence d'étudier la SSI selon une perspective individuelle de gestion des risques. Les influences sur les décisions des dirigeants pour la SSI confirment et prolongent les concepts théoriques de cette discipline. D'une part, les caractéristiques de l'évaluation psychologique des risques éclairent les biais pour la gestion du risque SI. D'autre part, l'étude de ces biais apporte une perspective nouvelle sur la compréhension de l'investissement des top-managers pour la SSI.

Nous montrons l'insensibilité des top-managers à l'exposition du risque, une préférence à aborder les risques sous l'angle des menaces. Aussi, nous exposons les influences qui contribuent à adopter une SSI technique et non managériale pourtant suggérée dans la littérature. Enfin, notre analyse fait émerger des perspectives pour prolonger la compréhension d'une SSI réactive, décriée par les auteurs en SSI.

***Mots clefs** : SSI, sécurité des systèmes d'information, influences, décision, risques, adoption symbolique, perception*

Abstract

The information system security (ISS) is a young discipline for which the interest joins in the increasing dependence of companies to them information system and in prospect of increasing number of security incidents. In this research, we are interested in the information system risk management, for whom the literature underlines the lack of involvement of top-managers.

Particularly, we approach the concern under the view of the decision of the top executives for ISS, through four theoretical streams: the models of the managerial perceptions of information system risks (Goodhue and Straub 1991; Straub and Welke 1998), the risks perception in psychology (Douglas and Wildavsky 1983; Fischoff and al. 1978; Sjöberg and al. 2004; Slovic and al. 1979; Wildavsky and Dake 1990; Yates and Stone 1992), the institutional theory (Di Maggio and Powell 1983; Scott 2005) and the theory about symbolic adoption of the innovations (Karahanna and al. 1999; Karahanna and Agarwal 2006; Klonglan and Coward 1970).

The aim of our works is to make intelligible the influences on the symbolic adoption of such ISS approach. Having adapted the model of symbolic adoption to the ISS, we use a qualitative method organized around 17 case studies in companies with varied activities. The ISS is then observed there as a process of decision for IS risks management. Our results highlight the relevance to study the ISS according to an individual perspective of risk management. The influences on the decisions of the top executives for the ISS confirm and extend the theoretical concepts of this discipline. On one hand, the characteristics of the psychological evaluation of the risks enlighten the biases for the management of the information system risk. On the other hand, the study of these biases brings a new perspective on the understanding of the investment of the top executives for the ISS. In particular, we underline the insensitivity of the top managers in the exposure of the risk, a preference to approach the risks under a threats point of view. So, we expose the influences which contribute to adopt a technical and not managerial ISS such as suggests by the Research. Finally, our analysis brings to the foreground perspectives to extend the comprehension of a reactive ISS, defame by ISS' academics.

Keywords : ISS, information security system, influences, decision, risks, symbolic adoption, perception

Remerciements

Ne cherchant pas l'exhaustivité, je vais répondre au délicat exercice des remerciements et m'adresser aux personnes qui auront été essentielles pour ce beau projet d'une vie.

Mes premiers remerciements sont adressés à **Leslie**, pour son soutien indéfectible, sa compréhension éternelle et sa patience infinie. Souligner que, sans elle, il n'y aurait pas eu ce travail doctoral serait un euphémisme…

Je tiens à remercier très sincèrement mon directeur de thèse, **Serge Amabile** pour son indulgence et sa persévérance. Conceptualiser les « complications » pour expliquer, retourner les faiblesses pour prolonger, gommer les défauts pour encourager, sont autant de ses capacités de chercheur en management. Je retiens particulièrement les nombreuses allégories, orientées et décalées, qu'il m'a exposées et qui m'ont autant éclairé que limé le cerveau.

Je souhaite également remercier **Bénédicte Aldebert** pour son extrême bienveillance, son humanisme et sa facilité à rasséréner. Ses apports durant ce travail doctoral ont été nombreux et ont dépassé la cadre méthodologique. Merci d'avoir écouté activement mes réflexions sur un sujet aussi « sexy » que la SSI.

J'adresse mes sincères remerciements aux membres du jury pour leur participation à l'évaluation de mon travail de recherche, **Professeur Sabine Carton** et **Professeur Claire Gauzente** pour avoir accepté de rapporter ce travail**, Professeur Cécile Godé Professeur Claudio Vitari** et **Emmanuel Houzé, Maître de Conférences Habilité à Diriger des Recherches,** pour avoir accepté de participer à ce jury.

Enfin, je remercie affectueusement les « personnes de l'ombre », **Nadine**, ma dévouée « assistante de thèse », **Jean-Yves**, maître à « pensée systémique », **Etienne**, « joyeux facilitateur » et **Dottore**, mon « cerveau d'accompagnement ».

Sommaire

Résumé **4**

Abstract **5**

Remerciements **6**

Sommaire **7**

Chapitre 1. Introduction générale de la recherche **9**

1.1. Contexte et objet de la recherche 9

1.2. Contributions et organisation de la recherche 20

Chapitre 2. État de l'art de la sécurité des SI **26**

2.1. Importance des SI 27

2.2. Sécurité du SI 30

2.3. Définitions du management de la sécurité de l'information 31

2.4. Principaux thèmes de la recherche en SSI 36

2.5. Prolongements théoriques de la recherche en SSI 76

2.6. Questions de recherche 82

2.7. Conclusion du chapitre 84

Chapitre 3. Cadre théorique pour l'adoption symbolique **88**

3.1. Le modèle d'adoption symbolique 88

3.2. Perception des risques 105

3.3. Influences externes et internes 187

3.4. L'adoption symbolique adaptée à la gestion du risque 193

3.5. Conclusion du chapitre 198

Chapitre 4. Épistémologie et choix méthodologiques **202**

4.1. Épistémologie 204

4.2. Méthodologie 219

Chapitre 5. Résultats de la recherche **234**

5.1. Contexte : SI et SSI 235

5.2. Les risques pour le SI, le dirigeant et l'entreprise 244
5.3. Influences isomorphiques 278
5.4. Éléments du processus de décision d'adoption symbolique 286
5.5. Réponse pratique au risque, mise en œuvre de la SSI 303
5.6. Commentaires des interviewés lors des entretiens 308
5.7. Synthèse des résultats de la recherche 310
Chapitre 6. Interprétations et discussions 314
6.1. Éléments considérés lors de la décision d'AS 315
6.2. Les influences sur la décision d'AS 342
Chapitre 7. Conclusion générale de la recherche 357
7.1. Les contributions théoriques de la recherche 358
7.2. Les contributions managériales de la recherche 362
7.3. Les limites de la recherche 365
7.4. Les voies de recherche 367
Bibliographie 368
Table des matières 388
Liste des figures 394
Liste des tableaux 395
Annexes 396

Chapitre 1. Introduction générale de la recherche

« Nous ne pouvons traiter que les risques que nous connaissons » énonçait le directeur d'un grand groupe français en avril 2018, pour expliquer qu'il ne « pouvait faire mieux ». Si, en tant que praticien de la **Sécurité des Système d'Information (SSI)** et, plus précisément, dirigeant d'une entreprise dont la principale activité est la « Gestion des risques », cette phrase peut laisser atone, elle paraît… une fois nos esprits recouvrés, pertinente et tout à fait opportune pour introduire nos travaux ! Ces dix mots désignent les principales clés théoriques et conceptuelles à partir desquelles sont architecturés les premiers chapitres de notre recherche : la SSI, son adoption symbolique et la perception des risques.

En effet, nous inscrivons nos travaux dans la discipline des systèmes d'information et, plus particulièrement, dans l'étude de leur sécurisation. La présente introduction développera donc le concept de **Système d'Information (SI),** les besoins des organisations qui y sont relatifs, les raisons motivant les besoins de protection des SI et, notamment, l'approche managériale nécessaire à la mise en œuvre de la SSI. Enfin, après avoir précisé notre problématique et nos questions de recherche, nous exposons les contributions attendues à travers ce travail doctoral.

1.1. Contexte et objet de la recherche

1.1.1. Les systèmes d'information

Depuis trois décennies, les évolutions du rôle des SI et des technologies utilisées dans les organisations sont étudiées. Plusieurs travaux indiquent ainsi un changement de « rôle » des SI, passant de « back office » à une position centrale pour les organisations non seulement en contribuant aux stratégies d'affaires mais aussi en permettant d'en créer (Henderson et Venkatraman 1992 ; McFadzean et al. 2007 ; Sambamurthy et al. 2003[1]). Les travaux réalisés dans cette perspective assurent notamment que « l'échange d'informations riches par des plateformes numériques, à l'intérieur et à l'extérieur des organisations, permet aux stratégies multifonctionnelles et aux processus d'être étroitement connectés » (Bharadwaj et

[1] Pour l'ensemble de ce document, lorsque cela sera nécessaire, les références bibliographiques seront présentées par ordre alphabétique.

al. 2013 p. 473). De fait, la stratégie numérique d'affaires se définit par l'articulation de la stratégie « informatique » et la stratégie d'affaires, sans aucune « distinction entre la stratégie d'affaires et la stratégie SI » (Peppard et al. 2014 p. 3). Les organisations qui inscrivent leur SI dans cette approche peuvent alors obtenir un avantage concurrentiel (Vitale 1986) en s'appuyant sur des SI alignés sur la stratégie de l'organisation (Doherty et Fulford 2006 ; McFadzean et al. 2007).

Toutefois, Peppard et Ward (2004 p. 168) indiquent que si « la plupart des organisations de tous les secteurs d'industrie, commerce et gouvernement dépendent fondamentalement de leurs systèmes d'information » elles « cesseraient rapidement de fonctionner si la technologie qui soutient leurs activités venait à s'arrêter ». En effet, cette dépendance des organisations envers leur SI implique l'utilisation croissante de technologies pour soutenir les aspects stratégiques et opérationnels de leurs activités (Gordon et Loeb 2002). Ces technologies sont souvent assorties d'un nombre important de vulnérabilités, pouvant être à l'origine de dysfonctionnements majeurs (Bandyopadhyay et al. 1999 ; Doherty et al. 2011). Les dysfonctionnements peuvent alors avoir des impacts sur l'activité des métiers supportés par le SI. Nous pouvons évoquer, sans chercher à être exhaustif, une perte de confidentialité de données personnelles impliquant une dépréciation de l'image ou des implications juridiques pour l'organisation (Dhillon et Torkzadeh 2006 ; Höne et Eloff 2002b ; Kwon et Johnson 2014) ou, encore, un problème de disponibilité des postes de contrôle industriels provoquant l'arrêt de la production (Doherty et Fulford 2006 ; Posthumus et Solms 2004 ; Straub 1990).

En tenant compte de l'éventualité de ces dysfonctionnements et des conséquences associées, il est largement admis que le fonctionnement du SI doit être sécurisé et pérennisé (Baskerville et al. 2014 ; Bulgurcu et al. 2010 ; Choobineh et al. 2007 ; Dhillon et Backhouse 2001 ; Posthumus et Solms 2004 ; Solms 2000 ; Spears et Barki 2010). Ainsi, la SSI doit offrir un certain niveau de résilience à la survenance des risques auxquels le SI est susceptible d'être exposé (Posthumus et Solms 2004). Nous inscrivons nos travaux dans cette perspective, d'une part, en regard de la dépendance croissante des entreprises envers leur SI (Backhouse et Dhillon 1996 ; Bandyopadhyay et al. 1999 ; CLUSIF 2014) et, d'autre part, en regard du nombre significatif d'incidents rencontrés chaque année (EMC 2015).

Nous focalisons nos travaux sur la contribution organisationnelle de la protection des SI et sous l'angle de la gestion des risques. En effet, nous distinguons les besoins de sécurité de l'organisation et les mesures techniques qui doivent être définies, puis mises en œuvre, pour y répondre. La littérature s'accorde unanimement sur la nécessité d'une **approche**

managériale et « métier » des risques SI (Karyda et al. 2005 ; McFadzean et al. 2007 ; Solms et Solms 2006b), plutôt qu'une approche technique dont les limites sont pointées dans plusieurs travaux (Dhillon et Backhouse 2001 ; Herath et Rao 2009a ; Taylor 2006). Solms (2000) précise ainsi que la SSI doit s'observer prioritairement comme une **problématique de gouvernance** et non pas comme une problématique de sécurité technique. Nous étudierons donc les décisions des directeurs et responsables métiers (que nous désignerons, dans ce travail, avec le terme « top-managers ») en ce qui concerne la SSI. Précisément, nous observerons les influences qui conduisent les top-managers à décider de la SSI, soit sur quels éléments ils proposent à leur organisation de répondre à ces risques pour éviter, ou le cas échéant limiter, leurs conséquences.

1.1.2. La protection des SI

Le concept de risque que nous mobilisons combine dans le même temps une menace et une probabilité de perte (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Dhillon et Torkzadeh 2006). Les SI sont exposés à différents risques. Premièrement, il y a les risques naturels comme les inondations, les incendies, les séismes, etc. Deuxièmement, il existe les risques de malveillance tels que le déni de service, le vol d'informations sensibles, etc. Enfin, nous retrouvons les risques liés à la cybercriminalité comme l'espionnage, l'activisme, le terrorisme, etc. (Loch et al. 1992 ; Straub et Welke 1998 ; Kayworth et Whitten 2010). Ainsi, comme l'indiquent plusieurs auteurs, le nombre et l'ampleur des incidents croissent chaque année (Bulgurcu et al. 2010 ; Gordon et al. 2005 ; Richardson 2008 ; Willison et Warkentin 2013).

Plus récemment, de nombreuses enquêtes rapportent l'**ampleur et les conséquences diverses liés à la survenance de ces risques**. L'étude « CSI Computer Crime & Security Survey » de 2014 (EMC 2014) indique que 4 organisations sur 5 ont vécu au moins un incident de sécurité et l'étude de 2015 en mentionne 79% (EMC 2015). En outre, 34% des répondants indiquent que le nombre d'incidents de sécurité a augmenté par rapport à 2013 et en 2015, 28% d'incidents de plus ont été détectés par rapport à 2014.

Dans l'ensemble de ces études, un incident de sécurité se définit comme une perte de service essentiel ou de données, ou encore une défaillance (Choobineh et Dhillon 2007). Dans cette définition, la perte de service et de données se traduit, *in fine*, par l'impossibilité pour l'organisation de délivrer les services reposant sur le SI. Selon PWC (2016), le coût moyen de chaque incident de sécurité serait de 2,5 millions de dollars et, à l'échelle mondiale (EMC

2015), le coût annuel des incidents de sécurité atteindrait 1700 milliards de dollars. **La tendance croissante de ces coûts** se relève aussi dans la littérature académique, avec un cout moyen par incidents évalué à 200 000$ en 2002 (Gordon et Loeb 2002), 500 000$ en 2008 (Richardson 2008) et entre 0,5 et 1M$ en 2016 (Whitman et Mattord 2016). Les conséquences de ces incidents sont définies par les impacts auxquels l'organisation doit faire face. Elles sont souvent associées à des pertes financières directes (Bagchi et Udo 2003 ; Choobineh et Dhillon 2007 ; Ma et al. 2008 ; Straub et Welke 1998), indirectes liées aux coûts de rétablissement du SI, ou encore au dédommagement des victimes (Bandyopadhyay et al. 1999 ; Baskerville 1993 ; Cavusoglu et al. 2004 ; Doherty et Fulford 2006). Ces conséquences peuvent également se traduire par des **pertes d'image** (Kayworth et Whitten 2010 ; Posthumus et Solms 2004 ; Solms 1999) et entrainer des **implications juridiques** (Eloff et Solms 2000 ; Höne et Eloff 2002b). Ainsi, un incident de sécurité majeur peut dépasser les seules pertes financières liées au SI, en obérant les objectifs stratégiques d'une organisation, tels que retarder le lancement d'un nouveau produit ou service ou, encore, empêcher son introduction en bourse (Solms et Solms 2005).

Pour donner une perspective aux conséquences des incidents de sécurité énoncées dans la littérature, nous présentons synthétiquement deux exemples qui illustrent les conséquences défavorables rencontrés par TV5 Monde et Ashley Madison en 2015 :

- TV5 Monde a vécu une cyberattaque qui a rendu impossible la diffusion des programmes durant plusieurs heures. Des hackers ont pris le contrôle de ses sites internet, de ses comptes sur les réseaux sociaux et de ses outils de production. Le coût pour reconstruire et sécuriser son infrastructure, d'un montant de 9,7 millions d'euros, a nécessité des arbitrages financiers qui ont eu pour conséquence « un appauvrissement des grilles de programmes »[2].

- Ashley Madison[3], site de rencontre canadien, a été victime d'un piratage de 37 millions de comptes alors que l'entreprise, selon elle, assurait « la sécurisation des

[2] http://www.senat.fr/rap/a15-168-4-4/a15-168-4-4_mono.html#toc63 (consulté le 27 août 2016). Notamment, le cout global est réparti entre quatre postes de dépenses : restauration du matériel endommagé, formation aux nouvelles pratiques de sécurité, acquisition d'équipements permettant de détecter les attaques et recrutement d'ingénieurs

[3] http://www.lemondeinformatique.fr/actualites/lire-ashley-madison-les-craintes-de-securite-des-dirigeants-du-site-62095.html (consulté le 10 décembre 2016)

> informations de ses abonnés »[4]. Pour l'entreprise, l'impact d'image est majeur, son introduction en bourse, prévue pour la fin de l'année 2015, a été annulée[5] et elle a dû faire face à des actions collectives d'utilisateurs et des autorités judiciaires américaines[6]. Pour les utilisateurs, cette fuite a eu pour conséquence une violation de la vie privée, a donné lieu à des chantages et au harcèlement en ligne. Il est à noter qu'une enquête interne a mis en évidence les préoccupations de sécurité du Président Directeur Général, du Directeur Technique Informatique et du Vice-Président Operations[2] et que des failles de sécurité avaient déjà été repérées, alors que la Direction Générale n'avait pas jugé utile de les corriger[3].

Historiquement, pour lutter contre ces incidents et assurer la protection des SI, les efforts des organisations sont généralement centrés sur les vulnérabilités des actifs technologiques tels que les matériels, les logiciels et les réseaux (Hu et al. 2007 ; Kayworth et Whitten 2010). Ainsi, les technologies de sécurité, qui permettraient alors de contrer les menaces auxquelles les SI sont exposés (Albrechtsen 2007 ; Dhillon et Backhouse 2001 ; Wood 1995), ont fait l'objet de nombreuses recherches. Cependant, la seule réponse technologique pour assurer la sécurité du SI est dénoncée dans de nombreux travaux (Dhillon et Backhouse 2001 ; Herath et Rao 2009a) alors que la prise en compte explicite des SI, des acteurs, des considérations métiers et des facteurs socio-organisationnels est présentée comme nécessaire (Zafar et Clark 2009). En d'autres termes, il s'agit d'inscrire la SSI dans une perspective managériale.

1.1.3. Le management de la sécurité de l'information

Selon plusieurs auteurs (Dhillon et Backhouse 2001 ; Solms 2000, 2006 ; Taylor 2006) la SSI mérite d'être positionnée au plus haut niveau de responsabilité des organisations. Solms (2000, 2006) inscrit ainsi la SSI dans le management en appuyant la nécessité qu'elle soit supportée par les directeurs et les top-managers, grâce à des structures organisationnelles appropriées, au travers de politiques, de processus et procédures. En effet, la sécurité dans une organisation est une fonction qui résulte de l'interaction entre les acteurs et la

[4] http://www.diplomatie-digitale.com/featured/surete/piratage-ashley-madison-reputation-1916 (consulté le 10 décembre 2016)

[5] https://www.entreprises-et-decideurs.fr/%E2%80%8BPirate-le-site-AshleyMadison-va-devoir-reporter-toute-introduction-en-Bourse_a728.html (consulté le 10 décembre 2016)

[6] http://www.lemonde.fr/pixels/article/2016/12/15/ashley-madison-va-payer-1-6-million-de-dollars-apres-le-piratage-de-36-millions-de-comptes_5049496_4408996.html (consulté le 10 décembre 2016)

technologie (Kayworth et Whitten 2010 ; Straub et Welke 1998) et nécessite de considérer aussi les facteurs socio-organisationnels pour être efficace (Hu et al 2007 ; Solms et Solms 2004a ; Spears et Barki 2010). Ces facteurs socio-organisationnels, contextuels à chaque organisation, peuvent être de plusieurs natures, tels que la culture sécurité (Hagen et al. 2008), les compétences et connaissances en SSI (Straub et Welke 1998), l'implication des acteurs (Spears et Barki 2010) et des directeurs (Hu et al. 2007) ou, encore, la maitrise des risques (Backhouse et Dhillon 1996 ; Dhillon et Backhouse 2001).

Ainsi, dans la perspective d'assurer la protection des SI, le management de la sécurité (MSSI) peut être présenté comme « la **conception**, la **composition** et le **reporting** des **structures organisationnelles de la sécurité de l'information** » auxquels s'ajoutent « les **rôles et les responsabilités**, les **compétences**, **l'expérience** et les **niveaux de ressources** engagées dans le dispositif de sécurité de l'organisation » (Da Veiga et Eloff 2007 p. 369).

En regard des enjeux, nous comprenons comment les questions relatives à la gestion des risques SI ont évolué d'une acception purement technique (Dhillon et Backhouse 2001 ; McFadzean et al. 2007 ; Soomro et al. 2016 ; Siponen et al 2014 ; Spears et Barki 2010) à une **problématique de gouvernance** (Da Veiga et Eloff 2007 ; Goodhue et Straub 1991 ; Karyda et al. 2005 ; Kayworth and Whitten 2010 ; Posthumus et Solms 2004 ; Solms et Solms 2006b). En ce sens, Solms et Solms (2005 p. 272) précisent que « dorénavant, de nombreux conseils d'administration intègrent la sécurité de l'information comme une partie intrinsèque de la gouvernance ». En effet, les responsables doivent prendre conscience de la criticité des ressources organisationnelles considérant ainsi la sécurité de l'information comme une activité sensible pour leur firme (Straub 1990 ; Ma et al. 2008). D'une part la réponse aux risques nécessite **un engagement de la direction** qui est **chargée d'engager la SSI** (Kotulic et Clark 2004 ; Straub et Welke 1998) et de contrôler globalement ces activités (de protection, Solms et Solms 2006a). D'autre part, les éventuelles conséquences d'un risque incombent aux managers exécutifs et au conseil d'administration (Choobineh et Dhillon 2007 ; Dlamini et al. 2009 ; Posthumus et Solms 2004). En effet, le top management doit assurer le succès de l'organisation et a donc la responsabilité de protéger ses SI (Goodhue et Straub 1991 ; McFadzean et al. 2007 ; Straub et Welke 1998).

Ces responsabilités sont représentées dans les travaux de McFadzean et al. (2007) qui synthétisent trois rôles majeurs structurant la gestion des risques SI : 1) rôle stratégique (définition des orientations et objectifs) ; 2) rôle institutionnel (acquisition des ressources et compétences) ; 3) rôle de contrôle (assurer la bonne déclinaison des actions managériales). Ces auteurs relèvent également que « **la perception des directeurs** de leur environnement

et, particulièrement, **la perception de risque, avait un impact sur ces trois rôles** » (McFadzean et al. 2007 p. 62). Ce constat s'inscrit dans la perspective des travaux de Bandyopadhyay et al. (1999 p. 440) qui précisent que « beaucoup d'organisations traitent le risque selon la perception de leurs directeurs » et qu'elles « n'emploient pas de méthode structurée pour évaluer le risque global ». Plus globalement, l'implication des directeurs est une condition incontournable pour la mise en œuvre d'une SSI adaptée (Barlette 2012 ; Goodhue et Straub 1991 ; Kotulic et Clark 2004 ; Straub et Welke 1998 ; Solms 2000, 2006 ; Solms et Solms 2006a). En effet, la décision d'engager la protection du SI nécessite une vision globale des activités de l'organisation, permettant d'identifier les potentielles conséquences des risques afin de définir et mettre en œuvre l'organisation pour y répondre (Barlette 2012 ; Boss et al. 2009 ; Bulgurcu et al. 2010 ; Solms et Solms 2006b). À l'inverse, l'absence de lignes directrices pour traiter les risques et de considération des managers sont susceptibles d'exposer l'organisation à des conséquences dommageables (Choobineh et Dhillon 2007).

En outre, il convient de relever, dans la perspective de formaliser notre problématique, que ces conséquences peuvent être catalysées lorsqu'elles s'accompagnent d'un ou de plusieurs des éléments suivants : la posture réactive des organisations face aux risques (Doherty et Fullford 2006 ; Kwon et Johnson 2014 ; Vance et al. 2014) et la faible implication des top-managers pour ce qui concerne la SSI (Kankanhalli 2003 ; Knapp et al. 2006 ; Straub et Welke 1998).

À propos du premier constat, le nombre important d'incidents de sécurité rencontrés par les organisations suggère qu'elles sont loin de réussir pleinement la mise en œuvre de leur SSI (Doherty et Fullford 2006 ; Hagen et al. 2008). Plusieurs auteurs soulignent ainsi que ces dernières sont souvent **mises en œuvre « après coup »**, c'est-à-dire que les organisations attendent de subir un incident pour initier l'analyse des contre-mesures possibles (Barlette 2012 ; Choobineh et Dhillon 2007 ; Goodhue et Straub 1991 ; Hagen et al. 2008 ; Kotulik et Clark 2004 ; Vance et al. 2014). Kwon et Johnson (2014) pointent pourtant l'importance de s'adapter proactivement aux risques car il semble inefficace de fonder l'apprentissage de la SSI selon des incidents dont il n'est pas certain qu'ils se reproduisent tout en en ayant toutefois subi les impacts.

En ce qui concerne le second constat, alors qu'il est admis, comme nous venons de l'évoquer dans les pages précédentes, que la sécurité de l'information est un problème de gouvernance, plusieurs travaux précisent que… **le top management investit peu la sécurité de l'information** (Kankanhalli 2003 ; Knapp et al. 2006 ; Straub et Welke 1998). Cela annonce

différents problématiques. Premièrement, de nombreuses recherches soulignent que la culture SSI des acteurs de l'organisation ne peut évoluer sans un investissement conséquent des « top-managers » (Knapp et al. 2006 ; May 2003 ; Siponen 2000). Deuxièmement, une SSI adaptée à l'organisation est efficiente dès lors que la décision provient du plus haut de l'organisation, soulignant l'importance accordée par la direction générale (Solms et Solms 2006b ; Mcfadzean et al. 2007). À l'inverse, Hu et al. (2007) précisent que **l'importance de protéger le SI peut être remise en cause par les collaborateurs de l'organisation** et manquer d'efficience en cas de faible mobilisation des dirigeants. Troisièmement, l'absence de considération des top-managers peut conduire à favoriser les aspects techniques de la SSI au détriment des enjeux et des besoins de protection des activités sensibles de l'organisation (Baskerville et Siponen 2002 ; Choobineh et Dhillon 2007 ; Zafar et Clark 2009).

Ainsi, en regard des implications de la SSI pour les organisations et leur fonctionnement, l'ensemble des éléments précédents marque l'importance d'explorer le rôle des directeurs et **leurs dispositions concernant la gestion des risques**.

1.1.4. Positionnement de notre recherche et problématique

Un des objectifs majeurs des directions générales est d'assurer que le fonctionnement de l'organisation ne soit pas obéré. Pour les SI, cet objectif se décline par la mise en œuvre d'un dispositif de sécurité global pour prévenir des pertes sur leurs activités organisationnelles (Anderson 2003 ; Dlamini et al. 2009). L'adaptation des dispositifs de SSI aux besoins des organisations a été un sujet de recherche pendant plusieurs années sous la rubrique d'analyse de risque (Straub et Welke 1998 ; Gordon et Loeb 2002). La recherche sur des technologies de sécurité telles la cryptographie, le développement de protocole sécurisé, la sécurité logicielle, les antivirus et les outils de détection d'intrusion, est aussi très fournie. Ainsi, la sécurité dans une organisation est une fonction qui fait interagir les utilisateurs avec la technologie, conduisant différentes études à s'intéresser à l'adoption de la SSI par les acteurs de l'organisation (Hagen et al. 2008 ; Zafar et Clark 2009). De nombreux travaux, permettant des avancées importantes sur cette thématique de la SSI, ont proposé plusieurs pistes de recherche. S'il y a un consensus dans la littérature sur la prise en compte globale des besoins de sécurité dans l'organisation, afin de disposer d'une protection efficace des SI et ainsi de l'activité des organisations, plusieurs auteurs relèvent, comme nous allons le voir, différents problèmes, voire dysfonctionnements.

Choobineh et Dhillon (2007) précisent que les organisations rencontrent des difficultés à mettre en œuvre une gestion des risques effective et efficiente. Ils évoquent la nécessité d'une compréhension plus profonde des défis des organisations pour la SSI. Précisément « le management de la sécurité de l'information est une discipline relativement immature qui exige des études académiques supplémentaires » pour alimenter la connaissance sur « les déficiences actuelles de management, identifiant les meilleures pratiques, concevant des méthodologies et spécifiant des exigences pour la gestion de sécurité de l'information » (Choobineh et Dhillon 2007 p. 959).

Crossler et al. (2013 p. 90) indiquent que les « recherches se centrent sur les problèmes techniques » pour expliquer que « **la faiblesse majeure dans la protection de l'information est l'humain** ». Ils appellent à explorer davantage les facteurs socio-organisationnels et notamment à « **distinguer la crainte en tant qu'émotion, de la crainte en tant que connaissance** ». Particulièrement, ils proposent d'étudier les comportements en SSI en mobilisant la **théorie culturelle de risque** (Douglas 1978 ; Douglas et Wildavsky 1983). Les travaux de Hu et al. (2007) s'inscrivent dans cette perspective. En effet, étudiant les influences organisationnelles externes et internes sur les actions organisationnelles pour la SSI, ils suggèrent de centrer les recherches sur les facteurs socio-organisationnels qui seraient contributifs à la compréhension des **déterminants importants de l'attitude envers la SSI**. Notamment, ils précisent l'importance d'expliquer **les comportements des directeurs pour la SSI**, comment leurs croyances et attitudes sont développées, et comment elles peuvent être influencées et changées (Hu et al. 2007 p. 155).

Liang et Xue (2009) ont développé un cadre théorique pour expliquer comment les utilisateurs perçoivent un risque SI et comment ils y répondent. Leur théorie est bâtie sur l'étude des conséquences pour les utilisateurs eux-mêmes et non pas pour leurs activités ou leur organisation. Albrechtsen et Hovden (2009 p. 486) s'inscrivent dans cette perspective en indiquant, pour la SSI, « **un manque d'études dans la littérature sur la perception du risque et la décision** ».

Backhouse et Dhillon (1996), Dhillon et Backhouse (2001) posent alors les questions sociales comme un composant central de la SSI et de l'analyse de risque. À l'appui de ces travaux, Baskerville et Siponen (2002) renforcent la nécessité d'ancrer la SSI dans le champ social afin, justement, de mettre en œuvre un dispositif de sécurité adapté aux enjeux de l'organisation et de ses acteurs. McFadzean et al. (2007) prolongent cette perspective et appellent à approfondir les recherches sur les structures de responsabilité, **la perception de risque** et des rôles formels et informels dans la SSI et, particulièrement, dans les processus

d'analyse de risque (Backhouse et Dhillon, 1996 ; Baskerville et Siponen, 2002 ; Dhillon et Backhouse, 2001). Ceci permettrait de comprendre davantage « le développement de la stratégie de sécurité de l'information et comment elle peut être convenablement alignée avec la stratégie d'entreprise » (McFadzean et al. 2007 p. 656).

De fait, si le risque SI et son appréhension restent **abstraits** (Tsohou et al. 2006) et **complexes** (Gerber et Solms 2005) pour les top-managers, certaines recherches montrent que les décisions de ces derniers sont influencées par plusieurs facteurs, dont les risques perçus (Boss et al. 2009 ; Bulgurcu et al. 2010 ; Soomro et al. 2016).

Ainsi, concernant les risques perçus et donc l'identification **des influences des décisions des top-managers s'agissant de la SSI,** Straub et Welke (1998) proposent un modèle de gestion des risques. La première étape de ce dernier relève de « l'identification et de la formulation de problèmes en ce qui concerne le risque SI ». Cette étape est fondamentale pour la mise en œuvre des quatre autres qu'elle précède (l'analyse de risque, la définition des solutions possibles, la décision de mettre en œuvre l'une d'entre-elles et, enfin, de l'implémenter, Straub et Welke 1998). De nombreuses recherches suggèrent ainsi que **l'identification des risques peut être tenue pour le point initial à partir duquel les décisions de gestion des risques sont prises** (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Choobineh et Dhillon 2007 ; Kotulik et Clark 2004 ; Mitchell 1995). Il est donc pertinent de s'intéresser aux **influences qui conduisent à l'initialisation du processus de gestion des risques**.

Nous inscrivant dans cette perspective, notre travail doctoral s'intéresse aux **influences qui sous-tendent la décision d'adoption de la SSI par les top-managers.** Précisément, nous nous intéressons à l'adoption conceptuelle de la SSI, afin d'explorer les influences sur la décision d'adopter la SSI, en écartant les besoins économiques et fonctionnels, soit en écartant la mise en œuvre de la SSI au sens de Straub et Welke (1998).

À cet effet, les travaux de Klonglan et Coward (1970) **éclairent les étapes dans le processus d'adoption**, permettant de distinguer l'adoption du concept de l'adoption d'usage, matérialisée par la mise en œuvre de l'innovation (Rogers 1983). En effet, l'**adoption symbolique (AS)** est un cadre théorique qui permet l'étude de « l'acceptation de la partie "'idée" d'une innovation, ou la décision qu'une innovation est appropriée » pour l'adoptant (Klonglan et Coward 1970 p. 82). L'AS a été développée et mobilisée pour explorer l'adoption ou le rejet d'une innovation pour laquelle l'incertitude est liée au manque

de connaissance d'une nouvelle pratique ou objet (Klonglan et Coward 1970 ; Karahanna 1999). Selon Klonglan et Coward (1970), le processus d'adoption comprend deux phases majeures que sont l'adoption symbolique, représentant l'acceptation de l'idée et l'adoption de « l'objet », représentant l'acceptation de l'objet matériel ou de la pratique (Klonglan et Coward 1970 p. 77). Karahanna et Agarwal (2006) expliquent ainsi que l'AS considère davantage les variables sociologiques pour expliquer « **l'acceptation mentale** », alors que les variables économiques peuvent être plus importantes pour expliquer l'usage (Rawstorne et al. 1998 ; Son et Benbasat 2007). Klonglan et Coward (1970) définissent l'AS selon trois phases (prise de conscience, renseignement et évaluation) qui, adaptées à la SSI, permettent d'étudier les risques pesant sur le SI, la connaissance de la SSI et les influences internes et externes pour y répondre (cf. figure suivante).

Les raisons précédentes soulignent l'intérêt de mobiliser le modèle d'adoption symbolique de Klonglan et Coward (1970) afin d'étudier les influences et leurs interactions sur l'identification des risques (Straub et Welke 1998).

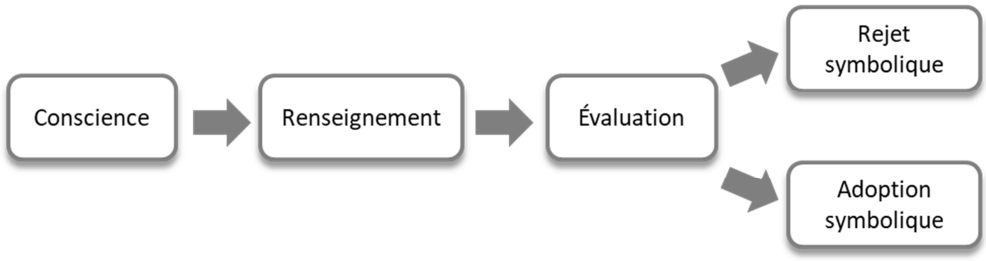


Figure 1 : Trois étapes conduisant au rejet ou à l'adoption symbolique
(Klonglan et Coward 1970 p. 80)

Notre recherche vise donc à comprendre les influences auxquelles sont exposés les top-managers pour mettre en œuvre la SSI. Si la littérature adresse l'implication des décideurs dans la SSI, il convient alors d'étudier les éléments qui structurent la décision des dispositifs de sécurité mis en œuvre dans les organisations, dont les influences externes et internes. Particulièrement, nous nous intéressons à la décision des top-managers d'adopter la SSI car nous souhaitons comprendre les éléments qui constituent en amont la décision de répondre (ou de ne pas répondre) au besoin de protéger le SI. Ainsi, notre problématique sera :

Quels sont les éléments considérés et leur influence sur
la décision d'adopter symboliquement la SSI ?

En effet, comme nous venons de le montrer, du fait du peu d'études portant sur la faible perception des risques SI des top-managers (Loch et al. 1992 p. 177[7] ; Kotulik et Clark 2004), il convient de saisir davantage la façon avec laquelle les top-managers décident d'investir la SSI. La perspective est de mieux cerner, de limiter, voire d'éviter les effets de certaines conséquences pour leur organisation et/ou pour eux-mêmes. Dans ce but, nous avons organisé notre recherche à partir de deux questions suivantes :

Quels sont les éléments considérés dans la décision d'adopter symboliquement la SSI ?

Comment ces éléments influencent la décision d'adopter symboliquement la SSI ?

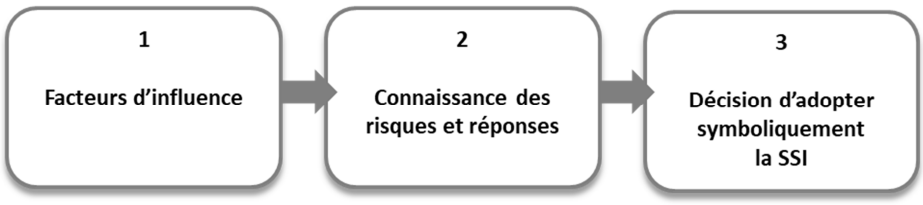


Figure 2 : Problématique de la recherche

1.2. Contributions et organisation de la recherche

1.2.1. Contributions académiques et managériales

Notre recherche vise à **identifier et comprendre les éléments considérés lors de la décision d'adopter symboliquement la sécurité des systèmes d'information**. Dans une approche exploratoire il s'agit alors d'articuler dans un cadre théorique de décision, les éléments considérés et leurs influences sur l'adoption symbolique (ou le refus symbolique) de la SSI.

Précisons que, pour le master recherche qui a précédé ce travail doctoral, nous avons conduit une étude sur « les fondements des politiques de sécurité des systèmes d'information » (PSSI). L'objectif de ces travaux a été d'observer des fondements des PSSI, soit quelles démarches les organisations utilisent pour les élaborer et quels principes de

[7] Loch et al. (1992) précisent la sensibilité du sujet de la sécurité qu'ils évoquent comme raison d'un faible retour à leurs questions pour lesquelles ils ont obtenu 20% de réponses.

sécurité sont précisés[8]. Neuf responsables de la SSI ont été interviewés. Nos résultats soulignent que l'investissement pour les PSSI repose principalement sur la sensibilité du secteur d'activité de l'entreprise et des personnes en charge de la sécurité. Aussi, bien que la PSSI soit centrale dans la construction du dispositif de la SSI, les top-managers ne semblent pas toujours concernés par le sujet. Ceci a aiguisé nos interrogations sur l'implication des top-managers et leur réflexion quant aux décisions pour la SSI. Ainsi, cette première étape de notre recherche a permis d'amener et de construire la problématique que nous développons dans ce travail doctoral.

Notre questionnement premier relève d'une part de la faible protection des SI des organisations (Straub et Welke 1998, cf. « 1.1 Contexte et objet de la recherche) et du manque d'implication des directeurs pouvant conduire à l'échec de la SSI d'autre part (Eloff 1988).

Nous inscrivons donc nos travaux dans le prolongement des études académiques établissant une relation entre la perception des risques et SSI. Parmi plusieurs études majeures, nous pouvons citer celles de Straub et Welke (1998) sur la faible perception des risques des top-managers, de Karyda et al. (2005) qui montrent la relation entre décision SSI et caractéristiques idiosyncratiques (expériences, connaissances, objectifs et priorités) ou, encore, de Tsohou et al. (2006) qui ont établi une relation entre théorie culturelle du risque et méthode pratiquée pour analyser et traiter les risques SI. Précisément, nous avons rappelé l'importance pour les organisations de réaliser un processus formel d'identification et d'analyse de risques, de façon à définir les mesures qui permettront d'y répondre. Ainsi, si la connaissance des risques est un résultat de ce processus, tel que mentionné dans le modèle de Straub et Welke (1998), nous proposons un **nouvel éclairage sur la décision d'engager ce processus**, soit les influences pour son adoption et par extension d'adoption de la SSI.

Précisément, notre contribution théorique repose sur une approche originale de la SSI. Elle combine dans un cadre fédérateur d'adoption symbolique, issu de la théorie d'adoption de l'innovation, la perception des risques, issue de la littérature en psychologie et l'analyse de risque, concept central à la SSI, pour donner un point de vue novateur mais complémentaire sur l'adoption de la SSI.

Le cadre théorique d'adoption symbolique, à l'appui de théorie de gestion des risques en SI, permettra de centrer nos observations sur **l'acceptation mentale de l'idée immatérielle**

[8] Le rôle et l'importance des PSSI sont précisés en détail dans la section « 2.4.3 Politique de sécurité des SI » p. 55)

de la SSI définie comme « variables sociologiques » par Klonglan et Coward (1970 p. 77). Cette théorie permet notamment d'écarter les « variables économiques », qui, a contrario des variables sociologiques, relèvent davantage de la matérialisation de l'idée après qu'elle ait été symboliquement adoptée (Klonglan et Coward 1970 ; Karahanna et al. 1999). Si de nombreux auteurs soulignent la posture réactive des organisations quant à la protection de leur SI (Choobineh et Dhillon 2007 ; Doherty et Fulford 2006 ; Goodhue et Straub 1991 ; Kotulik et Clark 2004 ; Kwon et Johnson 2014 ; McFadzean et al. 2007 ; Vance et al. 2014), à notre connaissance, la littérature est silencieuse sur les décisions pouvant conduire à une telle posture. Comme le soulignent Karahanna et al. (1999) dans le champ de la littérature en SI, l'adoption de la SSI est principalement étudiée pour les acteurs finaux, en n'observant que peu les motivations des décideurs pour la SSI.

En nous inscrivant dans cette perspective, nous souhaitons observer **les risques considérés** par les top-managers, sous l'angle de la connaissance nécessaire pour définir le dispositif de sécurité des SI. En effet, si l'analyse de risque est présentée comme l'étape incontournable pour mettre en œuvre la SSI, la littérature ne précise pas, à notre connaissance, comment est prise la décision de les analyser. Ainsi, explorer les influences qui peuvent concourir à la décision d'analyser les risques, soit la première étape de gestion des risques telle que définie par Straub et Welke (1998), peut contribuer à comprendre la posture réactive des organisations quant à la SSI et éventuellement d'identifier des perspectives académiques et managériales permettant une posture préventive.

Nous étudierons également **les influences externes** telles que définies par la théorie néo-institutionnelle et mobilisées par les auteurs en SSI (par exemple Knapp et al. 2009 ou Kwon et al. 2012) ou, plus globalement, sur le champ de la sécurité (Williams et al. 2009). L'étude des influences permettra d'éclairer les apports des normes qui s'imposent aux organisations ou encore des standards internationaux sur la décision d'adopter la SSI. Précisément, il s'agit de les positionner comme une influence externe, coercitive pour celles qui relèvent du règlement ou de la loi, ou normative pour celles qui serviraient de support à la réflexion.

Les contributions managériales portent principalement sur les éléments constituant l'adoption symbolique de la SSI. En effet, au-delà de la perception des risques par le décideur, la SSI nécessite une coordination de l'ensemble des acteurs de l'organisation. Goodhue et Straub (1991) montrent ainsi qu'un manque d'information sur les possibles impacts d'un risque peut induire une différence de point de vue entre top-managers pouvant conduire

certains de ces derniers à minimiser leur engagement pour la SSI. Nos travaux visent donc à mieux saisir la relation « décideurs – responsables métiers – experts en SI » de l'organisation afin de faciliter ou, du moins, de progresser vers une vision partagée des risques SI et de leurs potentiels impacts. Il s'agit précisément de rendre intelligible les influences considérées dans la décision pour faciliter les échanges « entrelacés » entre décideurs et managers tels que développées par Williams et al. (2009). Les influences sur la décision seront observées selon les risques qui impactent le dirigeant ou son organisation et son fonctionnement (Mitchell 1995 ; Moulton et Coles 2003).

Pour les décideurs, cela permettra d'observer si leurs expériences, connaissances, objectifs et priorités suffisent à élaborer une décision éclairée sur les risques et leurs impacts. Ils pourront arbitrer leur choix en regard des critères importants pour l'adoption symbolique de la SSI, selon chaque phase de la décision. Les managers, quant à eux, pourront activer ou non ces influences en fonction de leur propre perception du risque pour viser l'adoption symbolique de la SSI. Ils pourront davantage distinguer **les critères de la décision et améliorer l'efficience et l'efficacité de la promotion de la SSI**.

1.2.2. Posture épistémologique, Méthodologie et Protocole de la recherche

Notre recherche se positionne dans une **posture épistémologique constructiviste pragmatique.** En effet, notre projet ambitionne d'engendrer des connaissances théoriques ainsi que des connaissances actionnables. Précisément, en cherchant à cerner davantage et à décrire les influences prises en compte par les « top-managers » et conduisant à l'adoption symbolique de la SSI, nous souhaitons construire des connaissances scientifiques en nous concentrant sur l'étude de « phénomène » ou « artefact » au sens de Simon (1996). Pour ce faire, nous avons conçu notre recherche comme un **processus continu et dynamique**, constitué de multiples allers-retours entre terrain et théories, notre projet étant de présenter **une approche descriptive et compréhensive** des phénomènes étudiés. En d'autres termes, il s'agit de participer à l'intelligibilité des pratiques des acteurs, de présenter notre « point de vue sur le réel » (Le Moigne 2012).

Le choix de la méthode qualitative a été effectué au regard de ce paradigme épistémologique et de notre projet. En effet, l'objectif est d'utiliser les connaissances produites par des **études de cas** pour construire des connaissances actionnables, à partir des contraintes perçues sur le terrain. En ce sens, notre recherche s'inscrit dans une approche qualitative à visée

exploratoire, descriptive et compréhensive. Une méthode qualitative organisée autour de plusieurs études de cas est alors apparue pertinente.

Enfin, en cohérence avec les choix précédents, le protocole de la recherche a été organisé en deux étapes qui ont prolongé la construction d'une problématique débutée en amont de notre travail doctoral. Pour l'essentiel, la première a été constituée par une revue de la littérature en sécurité des systèmes d'information et par l'étude approfondie des travaux scientifiques développés autour de différentes théories, notamment, ceux concernant l'adoption symbolique et la perception des risques. Cela nous a permis de concevoir un guide d'entretien. Dans un second temps, souscrivant aux recommandations de Miles et Huberman (2003 p. 58), nous avons constitué un « petit échantillon » afin de pouvoir l'étudier en profondeur. Précisément, compte tenu de notre problématique portant sur la décision d'adoption symbolique de la SSI, nous avons sélectionné des acteurs disposant d'un niveau de **responsabilités au plus haut dans l'organisation**, tel que la littérature sur la SSI l'a explicité (cf. 2.4.1 « Gouvernance » p. 41) et **ne déléguant pas leurs décisions en ce qui concerne le management du SI et de sa sécurité**.

1.2.3. Organisation de la recherche

Nos travaux s'articulent autour de sept chapitres.

Le présent chapitre, l'introduction générale de la recherche, a permis de situer les SI dans leur contexte et leur importance pour les organisations. Ainsi, il a souligné la pertinence du sujet étudié. Il a donc proposé un aperçu liminaire mais global de la sécurité des systèmes d'information telle qu'elle est développée dans la littérature scientifique depuis une trentaine d'années. De même, l'intérêt de la recherche concernant la décision d'adoption symbolique des top-managers a également été mis en perspective. Ce premier chapitre a alors permis de présenter la problématique générale de la thèse ainsi que les théories mobilisées tout au long de la recherche.

Le deuxième chapitre parcourt les thèmes en SSI définis selon les travaux académiques issus d'une large revue de littérature. Après avoir précisément détaillé les définitions du management de la SSI, son évolution, de la technique vers des considérations socio-organisationnelles, les enjeux d'une vision holistique et globale sont précisés. Notamment, l'implication et l'importance de la participation des top-managers sont explicitées.

Le troisième chapitre aborde le cadre théorique de notre recherche, soit l'adoption symbolique issue de la théorie d'adoption des innovations. Nous adaptons ensuite ce cadre à notre étude sur la SSI et l'enrichissons des concepts issus de la littérature sur la SSI. Précisément, nous développons les concepts issus de la théorie néo-institutionnelle et de la perception des risques de la recherche en psychologie.

Le quatrième chapitre permet de présenter notre réflexion épistémologique et la méthodologie de recherche adoptée pour nos travaux.

Les cinquième et sixième chapitres sont dédiés, respectivement, à la présentation structurée de nos résultats puis à leur interprétation et à leur discussion.

Enfin, le septième chapitre, la conclusion générale, aborde les contributions théoriques et managériales de nos travaux, ainsi que les limites et les voies de recherche envisagées.

Afin d'éclairer notre approche de la recherche, un premier synoptique, sorte de canevas général de la thèse, faisant interagir problématique et questions de recherche, est présenté ci-après (figure 3).

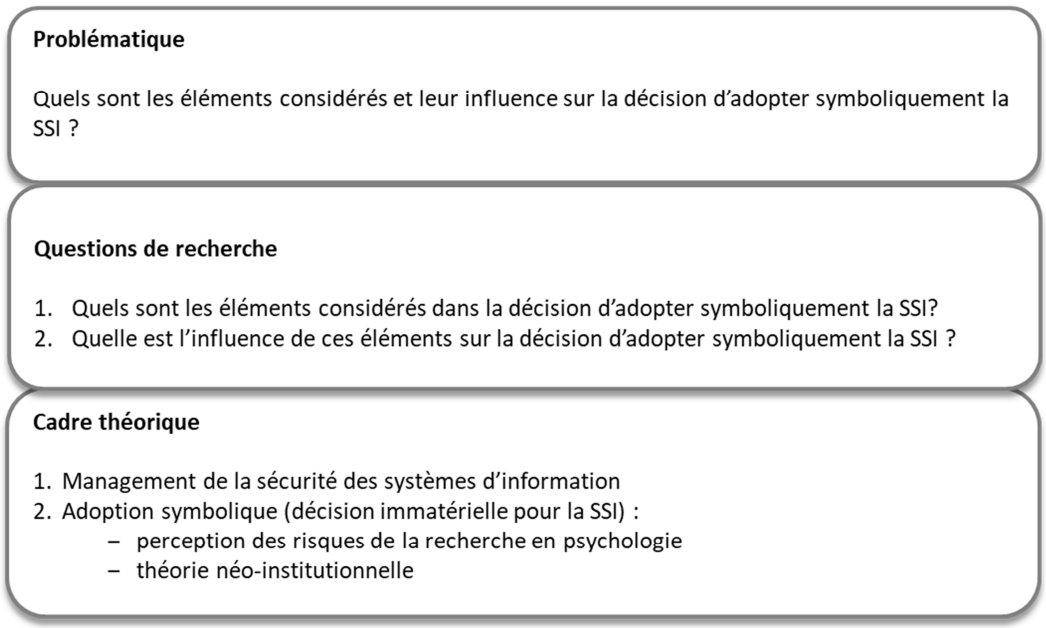


Figure 3 : Canevas général du projet de recherche

Chapitre 2. État de l'art de la sécurité des SI

« Les Romains firent, dans de tels cas, ce que se doivent de faire des princes sages, lesquels ont à se préoccuper non seulement des troubles présents, mais encore des futurs, et à y pourvoir de tous leurs soins : car en les prévoyant de loin, il est facile d'y porter remède, mais si on attend leur approche, le remède n'arrive plus à temps, parce que la maladie devient incurable. […] Ainsi vont les choses de l'État ; si l'on découvre de loin (ce qui n'est donné qu'à un homme prudent) les maux à leur naissance, la guérison est rapide ; mais faute de les avoir reconnus, on les laisse grandir à tel point que chacun les aperçoit, il n'y a plus de remède » (Il Principe, Machiavel 1515 p. 13, Éd Guy Trédaniel 2013)

Dans une large mesure, les prémices de la recherche sur le management de la sécurité des systèmes d'information (MSSI) sont centrées sur des aspects technologiques (Dhillon et Backhouse 2001 ; Gerber et Solms 2005 ; Spears et Barki 2010 p. 504).

Cependant, depuis deux décennies, un autre courant traite des aspects socio-organisationnels de la SSI. Il évoque notamment l'importance d'articuler les différentes approches de la SSI, techniques et organisationnelles, dans la perspective de disposer de systèmes d'information pérennes et fiables qui soutiennent les activités des organisations (Dhillon et Backhouse 2001 ; Dhillon et Torkzadeh 2006).

Au regard de ce constat, la **SSI est désormais considérée comme une discipline de gestion du risque** pour laquelle les décisions doivent être arbitrées au plus haut niveau des organisations (Hu et al. 2007 ; Kayworth et Whitten 2010). La SSI est devenue une problématique de gouvernance qui, dès lors, observe avec grande attention le spectre entier de l'organisation et de son environnement, assurant un niveau de protection des SI adapté à son fonctionnement et à ses enjeux. Attendu que nos travaux visent l'étude des influences sur la décision d'adopter symboliquement la SSI, nous exposerons dans le présent chapitre les raisons pour lesquelles, selon la littérature, les top-managers sont davantage impliqués pour les décisions de gestion des risques, évitant alors des conséquences défavorables pour l'organisation et pour eux-mêmes. Après avoir précisé l'importance des SI et de leur sécurité, nous dresserons les principales thématiques identifiées dans les revues de littérature SSI. Nous observerons ensuite les apports de chacune de ces thématiques pour nos travaux avant d'établir une synthèse des principales suggestions et propositions recensées dans la littérature.

2.1. Importance des SI

Désormais il est admis que le **SI se situe au cœur des activités des organisations** et se confond avec les processus fonctionnels et opérationnels (Bharadwaj et al. 2013). Son rôle majeur pour la création de valeur de l'organisation appelle à observer sa capacité à supporter ses processus. Ainsi, la littérature s'accorde à dire que l'IT (Information Technology) n'a aucune valeur inhérente et que seul le SI peut être une source d'avantage concurrentiel durable (Gerber et Solms 2005). Selon Sambamurthy et al. (2003 p. 253), « la valeur générée par l'IT repose principalement sur les stratégies d'affaires, les designs organisationnels, les structures et des compétences » positionnant ainsi les **SI comme stratégiques** (Kankanhalli et al. 2003). Ainsi, les investissements dans le domaine technique (IT) se justifient par leur influence sur les **performances en améliorant les capacités organisationnelles** d'une part, et en supportant la réalisation **des processus stratégiques** d'autre part (capacité d'innovation, actions entrepreneuriales et adaptation d'évolution) permettant alors d'obtenir un avantage concurrentiel (Kankanhalli et al. 2003 ; Sambamurthy et al. 2003). En effet, les SI supportent les activités principales des organisations s'ils sont alignés sur la stratégie de l'organisation (Doherty et Fulford 2006 ; Mcfadzean et al. 2007 ; Vitale 1986). Selon Bharadwaj et al. (2013), dans leurs travaux traitant de stratégie numérique (convergence des SI et de la stratégie), les organisations ont pris avantage des faibles niveaux de prix/performance et de la connectivité globale de l'IT pour adapter leur infrastructure d'affaires. Selon ces auteurs l'IT « **refaçonne fondamentalement la stratégie traditionnelle d'affaires** comme modulaire, distribuée, transversale dans des processus commerciaux globaux » (Bharadwaj et al. 2013 p. 472). Auparavant, Vitale (1986) expliquait l'intérêt accru des directeurs pour les SI sur la base des cinq forces de Porter. Aujourd'hui, les directeurs, sensibles aux potentielles utilisations concurrentielles, ne considèrent plus l'IT sous l'angle avantages / coûts mais en examinent les opportunités et se centrent sur leurs apports stratégiques (Kayworth et Whitten 2010). Loch et al. (1992 p. 184), deux décennies auparavant, associaient déjà IT et SI en indiquant que les organisations, dans le futur, devraient davantage s'appuyer sur l'IT pour « étendre les frontières » du SI pour « partager les informations et les ressources ». En synthèse, McFadzean et al. (2007) indiquent que l'évaluation de la contribution des activités conduites grâce au SI converge avec celle de la **performance organisationnelle**.

Notons les précisions de Dhillon et Backhouse (1996) qui, justement, indiquent que la **composante technologique du système d'information est souvent considérée à tort** comme le SI lui-même. Ainsi, pour Reix et al. (2011 p. 4), si le système d'information se

caractérise par « un ensemble organisé de ressources » comprenant « matériel, logiciel, personnel, données, procédures » dans le but « d'acquérir, de traiter, de stocker des informations dans et entre des organisations », il semble alors incontournable d'élargir la définition technique de la SSI à une vision plus englobante, a minima celle de l'organisation et de son environnement. Ces auteurs proposent une « définition amendée » du SI en introduisant l'articulation entre technologie de l'information et SI (« suite à une discussion avec Jean-Louis Le Moigne », op. cit) : « un système d'information est un système d'acteurs sociaux qui mémorise et transforme des représentations via des technologies de l'information et des modes opératoires » (Reix et al. 2011 p. 4). Ils concluent sur la finalité du SI en précisant qu'il « …est **imbriqué dans le fonctionnement et la structure d'une organisation** (liens étroits entre les processus de travail et le système d'information) » (Reix et al. 2011 p. 4).

Bandyopadhyay et al. (1999) soulignent la dépendance croissante à l'IT (et donc au SI) pour obtenir des avantages stratégiques. Peppard et Ward (2004) mentionnent que cette dépendance est fondamentale et que l'arrêt du SI **provoquerait l'arrêt des activités de l'organisation**. Backhouse et Dhillon (1996 p. 2) précisent que la SSI doit être considérée car « la dépendance répandue aux systèmes informatiques a provoqué ce changement dans l'intérêt *(pour la SSI)* pour des raisons pratiques évidentes ». Doherty et al. (2011) complètent ce constat en indiquant que les SI sont souvent assortis d'un nombre important de vulnérabilités pouvant être à l'origine de dysfonctionnements majeurs.

En effet, la littérature fait consensus sur le nombre et l'ampleur des incidents[9] survenus dans les organisations (Bagchi et Udo 2003 ; Dhillon et Backhouse 2001 ; Choobineh et Dhillon 2007 ; Goodhue et Straub 1991 ; Hu et al. 2007 ; Johnston et Warkentin 2010 ; Knapp et al. 2006 ; Ma et al. 2009 ; Whitman 2004). Selon plusieurs auteurs, avec un « faible niveau de sécurité de l'information », l'activité (de l'organisation) est exposée à **diverses conséquences négatives** telles que la perte de part de marché, l'incapacité de respecter des lois et des règlements, ou la perte d'image et de réputation (Fomin et al. 2008 ; Eloff et Solms 2000 ; Höne et Eloff 2002b ; Posthumus et Solms 2004 ; Solms et Solms 2005 ; Straub et Welke 1998). Pour compléter ce propos nous pouvons citer Ma et al. (2008 p. 252) qui indiquent qu'en plus « des pertes monétaires, les incidents de systèmes d'information peuvent aussi causer des dommages aux activités comme la **perturbation** de **processus**

[9] « Incident » tel que défini au paragraphe « 1.1.2 La protection des SI »

internes et de communication, la **perte de ventes** potentielles, la **perte d'avantage** compétitif et des **impacts négatifs** sur la réputation d'une entreprise, la **bienveillance et la confiance** ».

Les travaux de Bandyopadhyay et al. (1999 p. 440) explicitent la nécessité « d'adopter une **vue holistique et d'évaluer les menaces potentielles en considérant le spectre entier** de l'environnement informatique » de l'organisation. En effet, selon ces auteurs, la gestion des risques a jusqu'alors été parcellaire car limitée aux seuls logiciels informatiques (*« applications » dans le texte*), limitant la perception des impacts possibles en cas d'incidents (Bandyopadhyay et al. 1999). Ce constat a également été souligné par Loch et al. (1992) qui ont précisé que les managers SI considèrent le risque le plus élevé au niveau des « applications » en citant comme menace les catastrophes naturelles ou les mauvaises manipulations par les utilisateurs.

Nous avons évoqué dans l'introduction (paragraphe 1.1.2 La protection des SI) deux incidents ayant provoqué des pertes de différentes natures et ampleurs. Les aspects financiers (évalués à plusieurs milliards de dollars par Dhillon et Backhouse, 2001), révèlent une augmentation des pertes qui fait largement consensus. Ainsi, nous pouvons citer les chiffres de Johnston et Warkentin (2010), indiquant que la perte annuelle moyenne rapportée par des entreprises américaines a plus que doublée entre 2006 et 2007 (de 168,000 $ à 350,424 $). Hu et al. (2007) constatent que les attaques par virus et logiciel espion ou, encore, les infractions de sécurité sur les SI, semblent quotidiennes. Ces attaques aboutissent à des « pertes financières s'élevant au moins à des centaines de millions de dollars chaque année pour les entreprises américaines et probablement dans les 1000 milliards dans le monde entier » (Hu et al. 2007 p. 154).

Les conséquences d'un incident de sécurité, **portant alors principalement sur le cœur des activités et l'organisation elle-même**, nécessitent que les responsables d'affaires (autrement nommés responsables métier) contribuent à la définition des exigences de sécurité (Kayworth et Whitten 2010 ; Ma et al. 2009 ; Van Niekerk et Von Solms 2010). En effet il s'agit, pour ces responsables, de disposer d'une **vision globale des risques** qui pourraient **mettre en cause le fonctionnement des activités** lors de la survenance d'incident avec les potentiels impacts pour la société (Kwon et al. 2012 ; Soomro et al. 2016 ; Straub et Welke 1998).

2.2. Sécurité du SI

L'instruction générale interministérielle n°1300 SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale)[10] définit l'objectif général de la protection d'un système d'information comme étant de « garantir l'intégrité, l'authenticité, la confidentialité et la disponibilité des informations traitées par ce système. La protection d'un système d'information s'appuie sur des principes portant sur l'organisation et sur les moyens techniques… »[11]. Cet objectif de protection s'appuie sur le courant technique de la SSI, centré sur le respect des critères de sécurité dont les modèles historiques de contrôle d'accès sont issus (tel que par exemple celui de Lampson 1971, DAC[12] - Discretionary Access Control). Ces critères sont définis par la norme internationale ISO/IEC 27000 (2016) :

- Confidentialité : propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés
- Disponibilité : propriété d'être accessible et utilisable à la demande par une entité autorisée
- Intégrité : propriété d'exactitude et de complétude

En ce sens, Bishop (2003) **définit la sécurité** comme le **processus de protection** de la **confidentialité**, de l'**intégrité** et de la **disponibilité** de l'information. Whitman et Mattord (2009) précisent que ces trois critères, repris dans plusieurs normes internationales de sécurité, sont aussi connus comme un standard industriel nommé « le triangle CID » (Confidentialité, Intégrité, Disponibilité). Whitman et Mattord (2009 p. 8) soutiennent que la sécurité de l'information consiste en « la protection d'informations et ses éléments critiques, y compris les systèmes et le matériel qui utilisent, stockent et transmettent les informations ». Dhillon et Torkzadeh (2006) ont étudié les apports de la prise en compte des facteurs sociaux et organisationnels pour définir les mesures de sécurité. Ils concluent en « mettant en doute l'application généralisée des principes de confidentialité, d'intégrité et de disponibilité comme les pierres angulaires uniques dans la conception de la sécurité (Dhillon et Torkzadeh 2006 p. 312).

[10] L'instruction interministérielle n°1300 a pour objet de fixer les règles relatives à la protection des informations relevant du secret de la défense nationale

[11] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024892134

[12] Lampson, B. W. (1974). Protection. ACM SIGOPS Operating Systems Review, 8(1), 18-24.

En effet, considérer la SSI avec une lentille technique seule a été critiquée dans de nombreuses études (Albrechtsen 2007 ; Albrechtsen et Hovden 2009 ; Backhouse et Dhillon 1996 ; Dhillon et Backhouse 1994, 2000 ; Siponen et al. 2014 ; Solms 1996, 2000 ; Willison et Backhouse 2006). D'une part, pour Albrechtsen et Hovden (2009), les approches SSI définissent majoritairement des réponses mécaniques ne tenant pas compte des ressources humaines et de l'organisation. Ainsi, certains des verbatims de leurs travaux soulignent l'idée que les top-managers favorisent la protection du SI par la mise en place d'outils assurant le contrôle des utilisateurs et les sanctions lorsque les règles sont transigées (Albrechtsen et Hovden 2009). D'autre part, pour Spears et Barki (2010 p. 504) « il est largement admis que les efforts de l'organisation pour la SSI sont généralement axés sur les vulnérabilités des actifs technologiques **au détriment de la gestion d'autres sources de vulnérabilité, comme les personnes, les politiques, les processus et la culture** ». Dhillon et Torkzadeh 2006 p. 293), comme Taylor (2006), s'appuient sur des travaux antérieurs (Dhillon et Backhouse 2001 ; Straub et Welke ; 1998) pour souligner la nécessité « d'aller au-delà des moyens techniques pour protéger des ressources de l'information »[13]. Ces mêmes auteurs indiquent « qu'une part importante de la recherche sur la SSI est technique par nature avec une considération limitée pour les problèmes des personnes et des organisations » (Dhillon et Torkzadeh 2006 p. 293).

In fine, il semble donc que la SSI soit observée prioritairement sous la lentille technique pour deux raisons non exclusives : 1) **les menaces pesant sur le SI sont envisagées comme externes à l'organisation** (par exemple des virus ou des hackers) (Doherty et Fulford 2005 ; Whitman 2004) ; 2) les SI s'inscrivant dans le domaine technique (IT), la SSI relèverait alors par « héritage » **d'un problème purement technique**[14] (Posthumus et Solms 2004).

2.3. Définitions du management de la sécurité de l'information

Du fait des constats dressés dans la section précédente, il convient d'aborder la problématique de la protection du SI de l'entreprise en **considérant la combinaison**

[13] Bruce Schneier, célèbre expert de la sécurité et cryptologue illustre ces propos : « Si vous pensez que la technologie peut résoudre vos problèmes de sécurité, alors vous n'avez rien compris ni aux problèmes ni à la technologie » (https://www.ysosecure.com/securite-information.html consultée le 3 juillet 2018)

[14] Dhillon et Backhouse évoquent l'influence que « l'orientation mécaniste » a eu sur le développement des SI dans les organisations pour expliquer pourquoi les modèles qui en sont hérités "ignorent le contexte des actions sociales complexes dans lesquelles la technologie de l'information se développe » Dhillon et Backhouse 2001 p. 132).

organisationnelle (activités principales de l'entreprise, organisation et implication des acteurs) et **technique de la sécurité** (mise en œuvre des mesures technologiques de protection). Selon Zafar et Clark (2009) le management de la sécurité des systèmes d'information a plusieurs définitions. Les recherches en sécurité de l'information ont développé « des approches techniques, comportementales, managériales, philosophiques et organisationnelles qui adressent la protection et la réduction des menaces sur les biens informationnels » (Zafar et Clark 2009 p. 90). Avant d'observer le détail de ces définitions et les concepts qu'elles évoquent, nous pouvons dresser un historique synthétique de la SSI sur la base des travaux de Solms (1996 ; 2000 ; 2006). Selon cet auteur, la sécurité des SI a évolué en 4 temps, d'une considération technique vers une responsabilité de direction générale. Les quatre temps sont nommés « vagues » (Solms 2000 p. 615) et se définissent ainsi :

Vague 1 : la SSI ne concerne que l'aspect technique et relève de spécialistes en informatique. Il s'agit principalement de la sécurité des mainframes, basée sur le contrôle d'accès et les mots de passe.

Vague 2 : la SSI nécessite d'être gérée en tenant compte des aspects humains. L'essor du commerce électronique et du Web a eu pour conséquence l'intérêt des managers pour gérer la SSI. En effet, les SI deviennent centraux pour les activités métier des organisations, appelant alors l'attention des managers. Les structures organisationnelles formelles, les responsabilités et les politiques de sécurité de l'information sont définies, l'implication des acteurs pour la SSI est accrue.

Vague 3 : la SSI est standardisée pour être mieux contrôlée et démontrée. La SSI devient un facteur de communication et elle s'appuie alors sur les meilleures pratiques, la certification, le développement de la culture. Elle doit pouvoir être mesurée et contrôlée.

Vague 4 : la SSI est positionnée au plus haut niveau de responsabilité de la société, elle nécessite la considération managériale. Elle peut être définie comme la prise en compte explicite des SI avec la sécurité, devenant une partie intégrante d'une « bonne gouvernance d'entreprise », pour assurer la sécurité des systèmes d'information (Solms 2006 ; Zafar et Clark 2009).

Cette dernière évolution de la SSI dans les travaux de Solms, en considérant la problématique que nous développons, mérite une attention particulière. Cet auteur (Solms 2006 p. 167) établit les bases de la SSI sur :

- 1) « **l'engagement du board et du top management** »,
- 2) des « **structures organisationnelles appropriées** »,
- 3) les politiques, procédures, processus, technologies et mécanismes de contrôle de conformité.

En particulier, Solms appuie ses préconisations par le changement de paradigme des SI tel que nous l'avons introduit au paragraphe « 1.1.1 Les systèmes d'information » et développé au paragraphe « 2.1 Importance des SI ». Cela nous permet d'observer le parallélisme des changements IT et sécurité. D'une part, l'IT n'est plus considérée comme élément technique isolé mais comme SI, support majeur de la performance organisationnelle (Bharadwaj et al. 2013 ; Doherty et Fulford 2006 ; Kankanhalli et al. 2003 ; Mcfadzean et al. 2007 ; Sambamurthy et al. 2003 ; Vitale 1986). D'autre part, la sécurité du SI, traitée durant plusieurs années avec des réponses uniquement techniques (Baskerville 1993 ; Knapp et al. 2009), est maintenant articulée globalement dans et pour l'organisation, considérant davantage le management de la sécurité (Albrechtsen 2007 ; Choobineh et Dhillon 2007 ; Dlamini et al. 2009 ; Doherty et Fulford 2006 ; Karyda et al. 2005), avec des « politiques et procédures », des « programmes de sensibilisation », et des « mécanismes pour assurer la conformité » (Solms 2005 p. 445). Cette orientation de la SSI s'inscrit dans le développement d'Herath et Rao (2009a), articulant les activités des organisations et leur protection grâce à l'alignement des objectifs d'affaires et les exigences définies par la direction de l'entreprise.

Dans la littérature, les termes « management de la sécurité des SI » peuvent être définis différemment, selon le point de vue pris par le chercheur et son objet de recherche. En fonction du point de vue adopté, cette définition peut être orientée sous l'angle technique, comportemental, managérial, philosophique, et / ou organisationnel (Zafar et Clark 2009). Afin d'éclairer notre connaissance des concepts mobilisés par la recherche en SSI nous proposons une synthèse des définitions selon la littérature (cf. tableau 1). Notons que les auteurs n'énoncent pas systématiquement la définition du concept de la SSI dans leurs travaux, ce qui limite le nombre de définitions académiques formelles. Cette synthèse fait émerger une seule définition relevant du courant technique (Whitman et Mattord 2009). Les

autres s'inscrivent principalement dans un courant managérial, centrées sur les besoins de l'organisation (gestion des risques pour l'organisation et non pas pour le SI).

Définition de la SSI	Objectif des travaux	Référence
… fonction de l'organisation chargée de définir le scope et de réaliser les revues de sécurité (en s'appuyant sur un « programme » en 5 points 1 - Identifications des biens - informationnel ; 2 - Identification des vulnérabilités ; 3 - Évaluation des risques ; 4 - Identification, sélection et implémentation des protections ; 5 - Mise en œuvre du programme)	Critique des méthodes d'analyse de la SSI et articulation avec des méthodes plus globales	Baskerville 1993
« L'objectif est de **protéger des actifs** […] **des menaces** internes et externes pour que les coûts de **pertes** résultant de la réalisation de telles menaces soient **minimisés** »	Développer un cadre pour la gestion intégrée des risques IT	Bandyopadhyay et al 1999 p. 437
« … l'objectif principal est de maximiser la sécurité SI pour **protéger les ressources de l'information** de la société »	Développement des mesures de sécurité selon une approche socio-organisationnelle	Dhillon et Torkzadeh 2006 p. 296
« … est le processus pour administrer les gens, les politiques et les programmes avec l'objectif **d'assurer la continuité des opérations** en maintenant l'alignement stratégique avec la mission organisationnelle »	Identifier des défis pour le MSSI et argumenter la nécessité d'un nouveau développement théorique via l'examen de disciplines de référence	Choobineh et Dhillon 2007 p. 958
« … se réfère à un moyen de maintenir la sécurité des SI dans des organisations, incluant la planification et l'évaluation des SI. Ceci inclut aussi les questions de clé, de sauvegarde, du rétablissement et de la gestion d'éventualité. La confidentialité, la disponibilité, l'intégrité et la non-répudiation reniement sont les exigences pour la gestion de sécurité.	Identifier les approches retenues pour étudier la recherche en SSI	Siponen et Oinas-Kukkonen 2007 p. 62
Adresse tous « les aspects du management de la sécurité de l'information opérationnel » (contrôle des accès, pare-feux, anti-virus,…), « aussi bien que d'autres aspects liés à la création de politiques, de procédures, etc...)	Étude des différences qui devraient caractériser le management de la conformité de la SSI et la sécurité opérationnelle	Solms 2005 p. 444
« …est utilisé pour protéger tous les actifs de l'information de valeur et atténuer des risques divers pour ces actifs venant de tous les aspects de l'environnement de l'organisation en appliquant les technologies de sécurité et le processus de	Examen de l'influence de la culture d'organisation sur l'efficacité de mise en œuvre du management de la sécurité de	Chang et Lin 2007 p. 440

Définition de la SSI	Objectif des travaux	Référence
management »	l'information	
« … la nécessaire et juste combinaison des mesures qui **réduisent les risques commerciaux** à un niveau acceptable et assurent en même temps la **conformité à la loi** »	Étudier la mise en œuvre des mesures de sécurité de l'information organisationnelles et évaluer leur efficacité	Hagen et al. 2008 p. 379
« … processus d'identification des vulnérabilités dans le SI d'une organisation […] pour assurer la confidentialité, l'intégrité et la disponibilité de tous les composants du SI[15]	Définition des principes de la technique et du management de la sécurité des SI	Whitman et Mattord 2009 p. 118
« …est un processus continu d'identification et de priorisation du risque de sécurité informatique et la mise en œuvre et le contrôle de mesures (c'est-à-dire, des contre-mesures, des sauvegardes) qui adressent ces risques »[16]	Étude de la participation des usagers dans la gestion des risques SI et de son influence dans le contexte de la conformité réglementaire	Spears et Barki 2010 p. 505
« …préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate »	Exigences de mise en œuvre d'un système de management de la sécurité de l'information	ISO/CEI 27001 (2013) p. V

Tableau 1 : Définitions de la SSI identifiées dans la littérature

Au regard de la problématique que nous étudions, nous inscrivons **notre définition de la SSI dans l'approche socio-organisationnelle**. En effet, nous observons dans la littérature « qu'une proportion élevée des problèmes de sécurité sont le résultat d'erreurs, d'omissions ou d'abus commis par les employés d'une organisation » (Doherty et al. 2011 p. 201) et que les utilisateurs « sont souvent le maillon faible » de la SSI et considérés comme « la barrière la moins fiable pour prévenir l'incident » (Albrechtsen 2007 p. 277). Toutefois, nous souhaitons privilégier l'approche de Spears et Barki (2010) qui remarquent que si le **facteur humain peut être vu comme une faiblesse** pour la sécurité de l'information, **il peut devenir une force** si les rôles, les attributions et les principes sont clairement définis pour la SSI. En effet, notre vision de la SSI est adossée au commentaire de ces auteurs, nous

[15] La définition de Whitman et Mattord (2009 p. 8) est centrée sur les aspects techniques du SI « La protection d'informations et ses éléments critiques, y compris les systèmes et le matériel qui utilisent, stockent et transmettent des informations »

[16] Notons que Spears et Barki n'indiquent pas explicitement cette définition du MSSI mais une définition du management des risques et de la sécurité pour les SI.

conduisant à nous interroger sur l'implication des top-managers pour la SSI et plus particulièrement leur décision de l'adopter symboliquement.

Ainsi, notre recherche est centrée sur les éléments **de décision pour la SSI**, dont **nous retenons la finalité** : assurer la continuité des activités en protégeant les actifs informationnels (supports et données), afin de minimiser les impacts occasionnés par la survenance des risques auxquels sont exposés les SI (Bandyopadhyay et al 1999 ; Choobineh et Dhillon 2007). Nous définissons alors, pour l'ensemble de nos travaux, le risque comme étant les **conséquences défavorables, pour l'organisation, qu'une menace provoquerait en impactant le SI** (Posthumus et Solms 2004). Pour Choobineh et Dhillon (2007) le management de la sécurité de l'information est un processus de gestion des personnes, des politiques et des programmes permettant **d'assurer la continuité des opérations et conduit par des objectifs organisationnels**. Il s'agit alors, à un niveau stratégique de l'organisation, de mettre en œuvre une fonction dédiée à la gestion des risques SI (Anderson 2003 ; Dlamini et al. 2009 ; Posthumus et Solms 2004 ; Straub et Welke 1998 ; Solms 1999).

2.4. Principaux thèmes de la recherche en SSI

La difficulté d'établir une définition univoque de la SSI (Zafar et Clark 2009) peut refléter la diversité des acceptions revêtues par cette discipline. La SSI peut se définir par des acceptions stratégique, managériale et technique (Dagorn 2012), en accord avec son évolution, telle que présentée par Solms (1996 ; 2000 ; 2006). En effet, ce dernier a étudié la progression de la SSI, passant d'une considération technique et de spécialistes à une considération managériale et holistique (Dagorn et Poussing 2012 ; Dhillon et Torkzadeh 2006 ; Da Veiga et Eloff 2007), **positionnant aujourd'hui la SSI comme une réponse au risque SI, afin de satisfaire les besoins « métier » des organisations** (Karyda et al. 2005 ; McFadzean et al. 2007). Précisément, la SSI s'établit comme un besoin de gouvernance, permettant de spécifier les rôles et responsabilités de la gestion des risques SI (Knapp et al. 2009 ; Posthumus et Solms 2004 ; Straub et Welke 1998). Selon cette perspective, plusieurs auteurs décrivent alors la SSI dans les organisations selon un niveau stratégique, tactique et opérationnel (Da Veiga et Eloff 2007 ; Dlamini et al. 2009 ; Solms 1996, 2000, 2006 ; Solms et Solms 2006a). Ces trois niveaux mobilisés par plusieurs auteurs (Abrams et Bailey 1995 ; Da Veiga et Eloff 2007 ; Dhillon et Backhouse 1994, 1996), complétés des trois activités clés, sont définis dans le modèle « gouvernance et SSI » de Solms et Solms (2006, cf. figure 4).

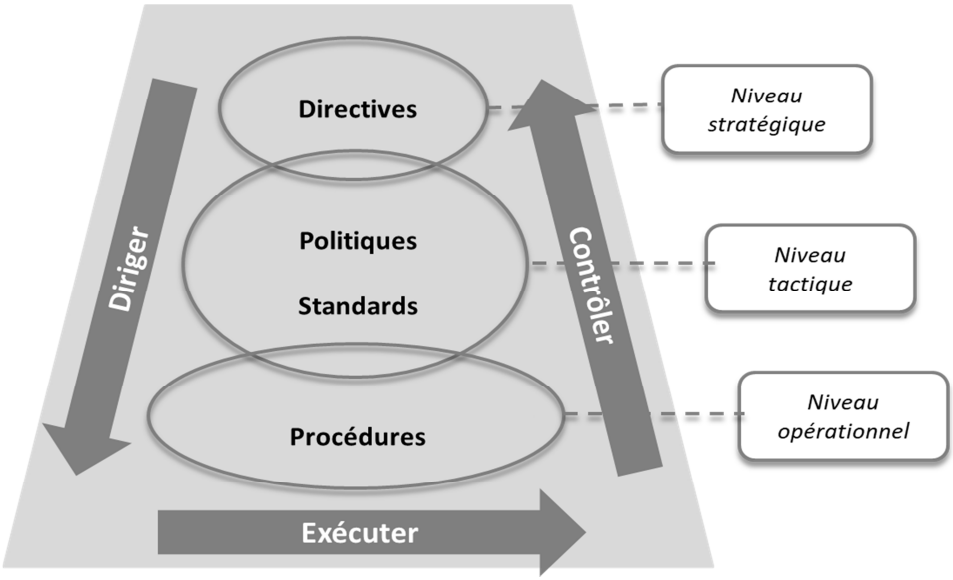


Figure 4 : Gouvernance et SSI, modèle de pilotage
(adapté de Solms et Solms 2006a)

En regard de notre objet de recherche, visant à explorer la décision d'adoption symbolique de la SSI par les top-managers, et en accord avec la position de Posthumus et Solms (2004 p. 638), nous constituons notre revue de littérature de la SSI comme une discipline qui traite la « gestion des risques, le reporting et la responsabilité », selon les niveaux stratégique, tactique et opérationnel. Particulièrement, nous observons cette définition de la SSI par niveaux, en perspective des rôles et responsabilités des top-managers, qui sont issus de la littérature. En effet, nous rappelons que McFadzean et al. (2007) définissent trois rôles structurant la gestion des risques SI (rôle stratégique, rôle institutionnel et rôle de contrôle, cf. 1.1.3 « Le management de la sécurité de l'information » p. 13). Ces rôles sont identifiés dans le modèle « gouvernance et SSI » de Solms et Solms (2006, cf. figure 4). Cette approche de la SSI, combinant niveaux d'étude et rôles des top-managers, nous permet de structurer la revue de la littérature en adéquation avec notre objet de recherche :

1. Niveau stratégique : vision des top-managers sur l'importance des actifs et orientation de la protection des SI de l'entreprise. Ces décisions sont basées sur plusieurs facteurs :
   - internes, tels que la vision stratégique de l'entreprise, le rôle du SI et son « alignement avec stratégie d'entreprise »
   - externes, tels que les risques et « les prescriptions légales et réglementaires » (op. cit.).

2. Niveau tactique : organisation de la SSI et gestion des risques, déclinaison de la politique de sécurité et des standards d'entreprise, alignés sur les orientations du niveau stratégique.
3. Niveau opérationnel : déclinaison en procédures des politiques et standards issus du niveau tactique. Ces procédures précisent les modes opératoires de la SSI dans l'organisation.

Notons que les trois niveaux d'étude de la SSI définis par Solms et Solms (2006) convergent avec les travaux de Da Veiga et Eloff (2007) sur le cadre de gouvernance de la sécurité de l'information (cf. figure 5). Ces auteurs déclinent ces niveaux en **plusieurs thèmes** d'études de la SSI :

- le niveau **stratégique** correspond aux définitions de « gouvernance et SSI » et de « management des risques », avancées par Zafar et Clark (2009 p. 587). Il s'agit des « structures de gouvernance », de la « stratégie de sécurité de l'information » et du « management des risques » (op. cit.). Nous traitons alors les structures de gouvernance et la stratégie de sécurité de l'information dans la section suivante de nos travaux et nommée « **gouvernance** ». Le management des risques concernent à la fois l'analyse de risques et leur traitement (Peltier 2004). Nous avons précisé au paragraphe 2.3 « Définitions du management de la sécurité de l'information » (p. 31), la relation étroite entre gestion du risque SI et mise en œuvre de mesure de sécurité pour couvrir les risques, objet de la finalité même de la SSI (Backhouse et Dhillon 1996). Aussi nous aborderons le management des risques dans le thème « **Analyse de risque** » et le traitement des risques dans le thème « **SSI et management** ». Enfin, Zafar et Clark (2009) précisent que la conformité relève d'une responsabilité de gouvernance, en accord avec (Solms et Solms 2006a p. 410) qui mentionnent pour ce niveau, la nécessité d'observer « les prescriptions légales et réglementaires ». La **conformité** étant un sujet d'étude étendu dans la littérature SSI[17], nous la traiterons, fidèlement aux propos de Solms et Solms (2006), comme un « facteur externe à l'entreprise » dans un thème dédié.
- le niveau **tactique** reprend les structures organisationnelles dédiées à la SSI que nous aborderons dans le thème « gouvernance » et « SSI et management ». La

[17] Le thème conformité, dans la littérature SSI, couvre la conformité des acteurs aux règles, la conformité aux standards, normes et bonnes pratiques, et la conformité réglementaire ou législative.

politique de sécurité, quant à elle, précise le fonctionnement et les responsabilités pour la SSI (Whitman et Mattord 2009) fait alors l'objet d'un thème dédié. Enfin les standards et, plus particulièrement, la conformité à leurs exigences, seront traités dans le thème « conformité ».

- le niveau **opérationnel** recouvre les modes opératoires pour la mise en œuvre pratique du management de la SSI. Ce niveau s'inscrit dans l'opérationnalisation de la SSI, soit le fonctionnement des activités « techniques » pour mettre en œuvre les mesures de sécurité SI. D'une part, ce sujet de la SSI n'entre pas dans le champ managérial dans lequel s'inscrivent nos travaux (Dhillon et Backhouse 2001). D'autre part, il s'agit d'une déclinaison « matérielle » de la SSI alors que notre étude vise à explorer son adoption symbolique soit l'acceptation mentale (Klonglan et Coward 1970). Enfin, si le volet opérationnel termine la constitution du dispositif de SSI de l'organisation, sa mise en œuvre est davantage sous la responsabilité de managers « techniques » que des top-managers. Pour ces trois raisons, nous n'abordons pas, dans notre revue de littérature, le niveau opérationnel de la SSI.

Notre propos n'est pas de structurer une revue exhaustive, issue de la convergence des travaux académiques sur les approches de la SSI mais plutôt de décrire les thèmes qui révèlent aux top-managers le cadre organisationnel pour assurer la protection des SI et pour lequel ils doivent arbitrer des choix.

Afin de vérifier la pertinence des thèmes retenus, nous avons synthétisé trois travaux dont l'objet est d'abordé les champs d'étude de la SSI. À notre connaissance ce sont les seuls[18] qui proposent une revue des thèmes de recherches en SSI dans des journaux reconnus [19].(cf. tableau 2). Notons que sur les trois articles identifiés, deux réalisent une revue des thèmes en SSI étudiés dans des journaux « sélectionnés dans les 10% les mieux classés » (Zafar et Clark 2009 p. 587).

[18] En complément, Dagorn (2012) a réalisé un classement des articles SSI en fonction des acceptions techniques, managériales et économiques, sans toutefois définir les thèmes qui y sont mobilisés

[19] Nom des revues et catégorie CNRS selon le classement 2017 : Zafar et Clark 2009: Communication of the AIS (4) / Silic et Back 2014 : Information Management & Computer Security (Non classée)/ Soomro et al. 2016 : International Journal of Information Management (3)

Thèmes de recherche	Gouvernance	SSI et management	Politique de sécurité des SI	Analyse du risque	Conformité
Zafar et Clark 2009	La gouvernance implique le développement stratégique et programmes de conformité qui aboutissent à un cadre robuste de management	Le management de la sécurité de l'information établit les structures de responsabilité qui contrôlent tous les aspects de l'organisation	Inclut toutes les politiques se rapportant à la sécurité de l'information et à leur effet global sur l'organisation	*Non abordé*	Compréhension et mise en œuvre de la conformité réglementaire, des contrôles et des audits sur la SSI
Silic et Back 2014	Définition de cadres, normes et politiques indiquant quelle stratégie doit être déclinée pour se prémunir des risques possibles	*Non abordé*	*Sous-thème de « Gouvernance »*	L'analyse de risque se réfère à l'analyse, la planification, la mise en œuvre, le contrôle et à la surveillance	Être conforme **avec toutes les exigences réglementaires**, légales et d'audit.
Soomro et al. 2016	La SSI est principalement une question de gestion et d'affaires, donc les directeurs devraient être **conscients de son importance**	Dans le passé, la SSI a **été traité comme une question technique** … sans permette une réponse suffisante à la problématique SSI	La **formulation de politique SSI** et sa **mise en œuvre** effective sont deux contributeurs principaux à l'efficacité de la SSI	L'analyse de risque inclut des approches d'évaluation qualitatives et quantitatives et pour définir des moyens pour contrer ces fragilités	La **conformité des salariés à la politique SSI** aura un impact positif significatif sur la SSI

Tableau 2 : Thèmes de recherche développés dans la littérature

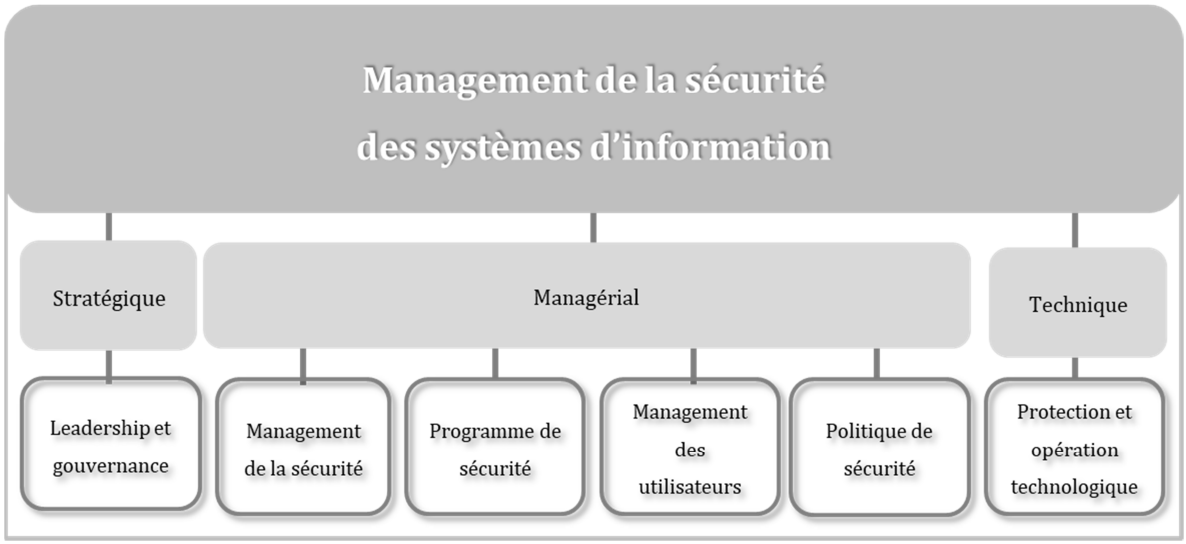


Figure 5 : Thèmes de recherche SSI
(adapté de Da Veiga et Eloff 2007)

Dans la section suivante, du fait de notre problématique concernant les éléments d'influence de la décision d'adopter symboliquement la SSI, nous présentons un état de l'art des principaux thèmes de recherches en SSI.

2.4.1. Gouvernance

Johnston et Hale (2009 p. 127) définissent la gouvernance comme « les **actions managériales des exécutifs,** indiquant la direction stratégique de la société pour la réalisation de ses objectifs, gérant les risques et les ressources de façon la plus effective et efficiente possible ». Ces mêmes auteurs déclinent cette définition à la SSI, précisant qu'il s'agit « d'un élément essentiel de la gouvernance d'entreprise et qui comprend le leadership, les structures organisationnelles et les processus traitant de la protection des biens informationnels » Johnston et Hale (2009 p. 127). Ils expliquent l'importance d'observer la SSI à un niveau de gouvernance car cela peut améliorer sensiblement les résultats pour la protection des SI. En ce sens et en regard de l'importance des SI, une des raisons personnelles pour laquelle les directeurs doivent intégrer la SSI au niveau gouvernance est précisée par Moulton et Coles (2003 p. 580), pour qui un « **échec à établir la gouvernance** effective *(pour la sécurité)* peut avoir des **implications sérieuses »** pour les top-managers,

alors que la mise en œuvre de moyens pour la SSI assurerait la démonstration de la rigueur suffisante pour préserver leur organisation et ainsi « **leur carrière serait sauvée ».**

Nous pouvons comprendre pourquoi un « échec » à établir le cadre permettant de traiter la SSI pourrait conduire à un processus moins efficace, ayant pour conséquence un niveau global de protection diminué, entrainant alors de potentielles conséquences négatives pour l'organisation. En effet, dès lors que la valeur et l'importance du SI sont significatives, c'est une responsabilité de direction générale que d'établir le cadre de la SSI (Solms et Solms 2006a). Hu et al. (2007) appuient ce propos en indiquant que l'intérêt et l'attention du plus haut niveau de l'entreprise est requis, car pouvant prendre en compte globalement des facteurs organisationnels et fournissant ainsi une défense significative contre les menaces. Pour expliciter ce constat, plusieurs travaux concluent que les éventuelles conséquences d'un risque incombent aux managers exécutifs et au conseil d'administration (Choobineh et Dhillon 2007 ; Dlamini et al. 2009 ; Posthumus et Solms 2004). En effet, le top management doit assurer le succès de l'organisation et a donc la responsabilité de protéger ses SI (Goodhue et Straub 1991 ; McFadzean et al. 2007 ; Straub et Welke 1998).

Pour Posthumus et Solms (2004 p. 644) les deux pans de la SSI, 1) gouvernance et 2) management, sont « les composants essentiels qui contribuent à une stratégie payante pour traiter le risque de l'information d'affaires » :

1. Il est exigé du conseil d'administration d'une organisation qu'il dirige et contrôle globalement et efficacement les orientations de l'organisation « ce qui inclut la SSI, puisque cela devient une partie fondamentale des opérations ». S'agissant des efforts pour la SSI, le conseil d'administration et le management exécutif doivent produire une politique de sécurité « corporate » qui démontre l'engagement et le support de la direction pour les missions, objectifs et stratégie de l'organisation.
2. Le management de la SSI adresse, quant à lui, « la façon dont les conditions (*pour la SSI*) sont mises en œuvre dans une organisation », impliquant « l'engagement des chefs de département pour implémenter les règles issues de la politique de sécurité de l'information d'entreprise » (traitant notamment des contrôles de sécurité appropriés qui peuvent permettre de préserver la confidentialité, l'intégrité et la disponibilité d'informations d'affaires). Enfin, les auteurs précisent qu'une fois « les mesures de sécurité mises en œuvre, les risques et contre-mesures choisies sont rapportés au niveau exécutif, leur permettant alors d'arbitrer les orientations SSI

> « de leur organisation avec la plus grande précision » (Posthumus et Solms 2004 p. 644).

Alors que pour Bandyopadhyay et al. (1999 p. 438) la dépendance croissante au SI « pour obtenir des avantages stratégiques pour l'organisation peut l'exposer à divers types risques » ne pas considérer cette problématique à un niveau de responsabilité de gouvernance est le premier des « péchés mortels du management de la SSI » (Solms et Solms 2004b).

Sur un autre aspect de l'organisation, Solms (2001b p. 217) précise que considérer la SSI au niveau gouvernance se justifie également par « l'utilisation d'une règle transitive simple, parce que la gouvernance d'entreprise inclut la responsabilité de contrôles internes solides et que ces contrôles internes reposent sur le SI, la SSI est une partie intégrante de la gouvernance d'entreprise ».

Pour Solms et Solms (2006), dans l'environnement d'entreprise d'aujourd'hui, où la valeur des SI est significative, la gouvernance fournit les principes de sécurité et le cadre dans laquelle une telle protection doit être assurée. Ces mêmes auteurs ont indiqué que ce cadre doit intégrer, les considérations éthiques et la confiance, pour définir une SSI globale et cohérente qui peut faire face aux risques (Solms et Solms 2005). Dans le prolongement de ces travaux, diriger et contrôler de façon holistique et efficace une organisation consisterait donc à intégrer les efforts pour diriger et contrôler la SSI comme une activité incontournable des opérations dans l'organisation » (Posthumus et Solms 2004). Pour Da Veiga et Eloff (2007) « définir les responsabilités pour la protection des SI consisterait à mettre en œuvre une approche globale de gouvernance pour la SSI ». Ils argumentent leur position en indiquant qu'« il est évident qu'une approche technique seule n'est pas suffisante pour manager la SSI, mais qu'une approche intégrée devrait être adoptée pour s'assurer que toutes les composantes relatives à la sécurité de l'information sont considérées. » Ce cadre de gouvernance pour la SSI agit comme « un point unique et global de référence pour le management de la SSI, articulant plusieurs composants pour limiter les risques sur les SI (Da Veiga et Eloff 2007 p. 371).

Enfin, Barlette et Fomin (2010 p. 126) constatent, à l'appui des études de Knapp et al. (2006) et de Chang et Lin (2007), que le support des cadres supérieurs influence positivement la culture de sécurité, la mise en œuvre et le respect de la politique, ce qui justifie l'engagement

managérial car « la direction générale a l'autorité et le leadership pour surmonter des barrières culturelles et organisationnelles ».

La gouvernance d'entreprise pour la SSI peut être considérée comme un sous-ensemble des SI. Ainsi, de façon comparable, en accord avec Solms (2001a), Moulton et Coles (2003) et Knapp et al. (2009), la gouvernance d'entreprise doit adresser plusieurs éléments pour la SSI : la stratégie et les objectifs, le management des risques SI, le respect des lois et règlements, le respect des règles et des relations avec les investisseurs et enfin, les activités de communications internes et externes. Particulièrement aux respects des lois et règlements, le conseil d'administration doit assurer que la gouvernance de l'organisation se traduise notamment avec un processus de gestion des risques assorti d'un système de contrôle interne efficace (Kayworth et Whitten 2010). En effet, de nombreuses obligations légales et réglementaires s'imposent au CA et aux directeurs, responsables s'ils échouent à respecter ces exigences (Humphreys 2008). S'agissant de la communication, McFadzean et al. (2007 p. 624) indiquent que « les investisseurs institutionnels prêtent davantage attention aux pratiques de gouvernance des sociétés dans lesquelles ils investissent, cherchant des pratiques de gouvernance comme une indication positive d'un centre de valeur pour les actionnaires ». En ce sens, Zafar et Clark (2009) soulignent que les organisations ne seraient pas encouragées à adopter la SSI, justement parce qu'elles n'auraient pas l'obligation d'informer les parties prenantes des incidents rencontrés.

Pour Dlamini et al. (2009) la problématique SSI se situe désormais dans une approche plus stratégique, s'intégrant à la gouvernance des sociétés, notamment parce que la SSI nécessite une approche pluridisciplinaire (affaires, managériale et technique). En ce sens Posthumus et Solms (2004), s'appuyant sur l'impossibilité d'assurer la protection du SI par une solution technique seule, indiquent que la SSI ne peut être autre que stratégique. Cette nécessité est renforcée par d'autres auteurs qui indiquent que seule la direction générale peut définir et contrôler les processus de gestion des risques et de mise en œuvre des contre-mesures, dont ils ont, in fine, la responsabilité (Moulton et Coles 2003 ; Posthumus et Solms 2004 ; Solms 2001a ; Straub et Welke 1998). Précisément, Moulton and Coles (2003 p. 580) recommandent que la sécurité soit traitée au niveau de la gouvernance, ce qui permettrait « d'établir et maintenir un environnement de contrôle adéquat », assurant que « les directeurs identifient les risques "'informationnels" au niveau d'entreprise ». Ils complètent leur recommandation en indiquant que ces risques sont gérés par des responsables assignés selon des processus de contrôles appropriés. Cette recommandation est comparable à celle de Soomro et al. (2016) qui indiquent que les directions générales peuvent orienter la SSI en

fonction des choix stratégiques décidés pour la société, en y incorporant les « changements et nouveaux défis » auxquels elle fait face.

Pour synthétiser les raisons du positionnement de la SSI au niveau de la gouvernance, nous nous appuyons sur les travaux de McFadzean et al. (2007 p. 3). Selon ces auteurs la SSI est un sujet trop important pour être délégué sans un contrôle rigoureux de la direction. Ils indiquent, que généralement, ce positionnement de la SSI relève de 6 raisons principales :

1. **Autorité** : Les directeurs ont l'autorité suffisante sur l'ensemble des actions permettant de construire le dispositif de protection, sa mise en œuvre et ses processus de contrôle et d'audit. Selon Kankanhalli et al. (2003) l'implication des top-managers est fondamentale pour que les responsables en charge de la mise en œuvre n'aient pas de difficulté à imposer les plans de sécurisation (actions relatives aux politiques, ressources, formation, communication, contrôle, etc.)
2. **Leadership** : « La SSI devrait être une partie intégrante de la culture d'entreprise. Autrement dit, le personnel devrait automatiquement employer des processus de sécurité de l'information dans leur travail quotidien. Si les salariés et autres parties prenantes écartent les principes de sécurité de l'organisation » alors le dispositif de sécurité est en défaut. Selon Solms (2001a) la culture SSI n'est établie qu'à la condition d'un engagement complet de la direction générale et des top-managers.
3. **Responsabilité de gouvernance** : Dans le cadre de leurs obligations relative à la gestion du risque, les directeurs sont in fine responsables du développement de la SSI. En effet, la SSI nécessite une large organisation d'éléments que seuls les directeurs peuvent exiger (tels que par exemple la définition d'une structure organisationnelle appropriée, l'établissement de politiques et l'affectation des ressources). Ce rôle est désormais incontournable compte tenu du renforcement des règlements et législations tels que Sarbannes-Oxley par exemple (Peltier 2004). De plus, les directeurs peuvent aussi communiquer aux salariés de toute l'organisation les processus et les procédures sécurité qu'ils doivent respecter (Solms 2001a). Solms et al. (1994) prolongent cette recommandation en indiquant que communiquer ce fonctionnement aux parties prenantes externes peut contribuer à la confiance qu'ils accordent à la société.
4. **Vision** : La vision holistique des directeurs leur permet d'évaluer l'importance des SI et des dommages potentiels pour l'organisation en cas d'incident. Notons que selon Willison et Backhouse (2006) le budget nécessaire à la SSI ne peut être correctement

engagé par la direction générale que lorsque celle-ci dispose d'une compréhension claire de la complexité de la SSI.

5. **Bonne pratique de management** : C'est la responsabilité du conseil d'administration de garantir l'adéquation du personnel, de la technologie et des SI pour assurer que l'entreprise reste compétitive (Solms 2001a). Par conséquent, alors que les processus technologiques et de sécurité deviennent plus sophistiqués, c'est la responsabilité du conseil d'administration d'assurer que la technologie est tenue à jour et qu'elle reste aussi sécurisée.
6. **Gouvernance, sécurité et SI** : Il est maintenant largement accepté qu'un bon niveau d'alignement entre les ressources de l'information d'une organisation et sa stratégie d'affaires peut être une source significative d'avantage compétitif. Ainsi, parce que le conseil d'administration engage les questions de gouvernance SI, il doit aussi être impliqué dans les sujets traitant de la sécurité du SI.

La littérature existante sur la SSI comprend de nombreuses études suggérant la nécessité d'aborder cette question globalement, en tenant compte, notamment, des besoins « métier » des sociétés (Soomro et al. 2016 ; Solms et Solms 2005). Nous avons observé un consensus sur la nécessité de traiter la SSI comme « problématique d'affaire », et non pas une question technique, s'agissant alors d'une responsabilité relevant de la gouvernance (Da Veiga et Eloff 2007 ; Eloff et Solms 2000 ; Höne et Eloff 2002b ; Kayworth et Whitten 2010 ; Knapp et al. 2009 ; Kwon et al. 2012 ; Posthumus et Solms 2004 ; Solms 2001,2005, 2006 ; Solms et Solms 2005). En ce sens, pour Kwon et al. (2012), la démarche pour assurer la SSI implique de donner la priorité à la protection des informations supportant la stratégie d'affaires de l'organisation. Pour ces mêmes auteurs, le manque d'intérêt pour diriger la SSI relève d'un « échec de gouvernance », ne permettant pas de répondre prioritairement aux vulnérabilités des SI (Kwon et al. 2012), exposant ainsi les sociétés à différentes conséquences (telles que développées aux paragraphes 2.1 Importance des SI) (Doherty et Fulford 2006).

Si pour plusieurs auteurs les conseils d'administration sont de plus en plus contraints d'incorporer la SSI comme une partie intrinsèque de la gouvernance (Solms et Solms 2005 ; Eloff et Solms 2000 ; Höne et Eloff 2002b), de « préférence intégrée dans les processus qu'ils ont mis en place pour régir les SI » (Solms et Solms 2005 p. 272) et que les responsables en ont pris conscience parce que les SI sont des « ressources organisationnelles critiques » (Straub 1990 p. 255), ils devraient considérer la SSI comme une activité cruciale pour

l'organisation. Cependant Kayworth et Whitten (2010) indiquent qu'à cause du manque d'alignement entre la stratégie d'affaire et la SSI, les politiques de sécurité et les budgets sécurité des sociétés ne reflètent justement pas les besoins réels. Pour ces mêmes auteurs, diminuer le nombre d'incidents de sécurité nécessite un meilleur alignement SI / SSI, en articulant la stratégie de sécurité sur la stratégie organisationnelle.

En ce sens Eloff (1988) s'est interrogé sur la mise en œuvre de programme de sécurité en s'appuyant sur le constat d'une atteinte partielle des résultats attendus. Ceci a initié la question « quels sont les facteurs critiques de succès et d'échec dans la mise en œuvre de la sécurité informatique ? » (Eloff 1988 p. 559). Nous trouvons pertinent d'indiquer les réponses possibles, attendu que des commentaires comparables sont indiqués dans de nombreuses études, plus de vingt ans plus tard. Eloff (1988 p. 559) indique deux raisons majeures à l'échec des programmes de sécurité :

1. **Manque de participation de la direction générale** car la « sécurité informatique » est une terminologie indiquant qu'il s'agit d'un problème qui incombe au seul « département informatique »,
2. La recherche et la pratique ont centré les aspects de sécurité informatique « **sur la technique**, par opposition au managérial ».

Dlamini et al. (2009) introduisent une notion dans la compréhension des organisations quant à la mise en œuvre de la SSI. Ils précisent que « **pendant longtemps la plupart des organisations n'ont pas reconnu l'importance de sécuriser** leurs informations stratégiques. La sécurité de l'information a été traitée comme un sous-produit, comme "un mal nécessaire qui gêne la productivité". **Les organisations le feraient simplement parce que toutes les autres le font »** (Dlamini et al. 2009 p. 2). Pour Kankanhalli et al. (2003) le faible engagement managérial pour la SSI peut s'observer en regard de la nature et du nombre d'incidents que rencontrent les organisations.

Choobineh et Dhillon (2007 p. 961) indiquent que le management de la SSI fait face à plusieurs défis majeurs : 1) « même après les décennies de recherche dans la théorie et la pratique de la sécurité informatique, on considère d'habitude **le management de la sécurité après coup** » et 2) « … parce que l'on considère la sécurité après coup, le problème de développement (*de la SSI*) est une dualité » (la SSI n'est pas prise en compte durant le développement des SI mais après). Notons ici que si les commentaires sur la mise en œuvre d'une sécurité réactive sont reportés par plusieurs auteurs (Barlette 2012 ; Choobineh et

Dhillon 2007 ; Hagen et al. 2008 ; Kotulik et Clark 2004 ; Vance et al. 2014), Kwon et Johnston (2014) ont démontré que des investissements préventifs pour la SSI avaient pour conséquence une baisse des incidents rencontrés.

Hu et al. (2007 p. 162) indiquent, pour une des entreprises interrogées, qu'elle aurait mis en œuvre un dispositif de sécurité plus adéquat si « l'entreprise avait été piratée ou s'il y avait eu un **incident dans lequel les numéros de carte de crédit** avaient été volés, ceci pourrait avoir été un **catalyseur** pour mandater et formaliser la sécurité des procédures à mettre en place ».

En ce sens, Solms et Solms (2006) remarquent, qu'au niveau le plus haut de l'organisation, l'importance du SI et sa protection, puis son articulation avec la vision stratégique de l'entreprise sont des décisions basées sur plusieurs facteurs :

1. externes : les prescriptions légales et réglementaires ainsi que différents risques
2. internes : la vision stratégique, le rôle des SI, l'alignement du SI avec la stratégie d'entreprise

Selon la définition de la gouvernance pour la SSI, une fois établis les principes directeurs de la sécurité, il appartient justement aux directeurs et top-managers de les traduire au niveau managérial (Posthumus et Solms 2004). Nous rappelons que les bases de la SSI sont « l'engagement du board et du top management » et les « structures organisationnelles appropriées » (Solms 2006 p. 167). Ainsi, nous abordons plus précisément le rôle des directeurs et des top-managers dans les décisions relatives à la déclinaison des « structures organisationnelles appropriées ». En effet, selon plusieurs auteurs le rôle des directeurs est majeur dans la décision et la mise en œuvre de la SSI (Barlette et Fomin 2010 ; Boss et al. 2009 ; Bulgurcu et al. 2010 ; Chang et Lin 2007).

McFadzean et al. (2007 p. 637) ont trouvé « que les membres des conseils d'administration ne développent pas de stratégie SSI » mais sont dans des dispositions à « revoir et valider les propositions faites par les top-managers ». Nous avons présenté des raisons pouvant expliquer le faible engagement des directeurs et top-managers (Eloff 1988 ; Posthumus et Solms 2004 ; Solms 2006), qui se recoupent avec celles indiquées par McFadzean et al. (2007) :

1. les membres du conseil d'administration trouvent difficile la compréhension du langage technique employé par les spécialistes en SSI,

2. les conseils d'administration voient la SSI comme « opérationnelle » et préfèrent la déléguer aux spécialistes de sécurité dans leurs organisations.

Les travaux de McFadzean et al. (2007) démontrent que l'engagement des directeurs pour la SSI prend en compte leur perception de leur environnement **et particulièrement la perception de risques**.

Nous développerons, dans le prolongement des concepts énoncés dans le thème « gouvernance », les résultats des travaux en sécurité de l'information et management, traitant justement de l'approche développée pour la SSI par les directeurs et top-managers, le management de la sécurité de l'information.

2.4.2. Sécurité des systèmes d'information et management

En regard de la définition de Solms (2005) pour la SSI, nous nous intéressons à la littérature traitant de la définition et de la mise en œuvre des « structures organisationnelles » de la SSI.

Le management de la sécurité de l'information a été critiqué pour être centré sur les aspects technologique (Baskerville 1993 ; Gerber et Solms 2005 ; Knapp et al. 2009). S'il est largement admis que les efforts de l'organisation pour gérer la sécurité sont généralement axés sur les actifs technologiques, il est maintenant incontournable **d'organiser globalement la protection du SI** (Albrechtsen 2007 ; Choobineh et Dhillon 2007 ; Dlamini et al. 2009 ; Doherty et Fulford 2006 ; Karyda et al. 2005). D'une part la technologie axée sur la SSI est généralement concentrée sur les seules menaces extérieures, telles que les virus et les pirates (Doherty et Fulford 2005 ; Whitman 2004), alors que les organisations sont également exposées aux malveillances internes (Spears et Barki 2010 p. 504). D'autre part, l'approche managériale de la SSI peut répondre aux **exigences de l'organisation** pour prendre en compte **les spécificités des organisations et de leurs activités**, permettant, alors, de disposer d'une réponse adaptée (Hu et al. 2007). Spécifiquement, l'adéquation de ce dispositif de sécurité reposerait sur son alignement avec les objectifs d'affaires (Herath et Rao 2009a).

Baskerville (1993) a montré les limites des méthodes jusqu'alors utilisées pour la SSI, centrées sur les technologies et destinées à des spécialistes, pour appeler à l'emploi de méthode d'autres domaines, afin d'intégrer la SSI plus globalement dans l'organisation. De façon similaire, Backhouse et Dhillon (1996) ont critiqué les approches SSI pour développer

un cadre conceptuel alternatif permettant de tenir compte des spécificités de leurs domaines d'application. Dans la suite des auteurs critiquant les « méthodes classiques pour la sécurité », Choobineh et Dhillon (2007 p. 958), précise leur inadéquation avec les fondamentaux de la SSI : « le management de la SSI peut seulement être assuré de façon adéquate si l'accent va au-delà des contrôles techniques et incorpore les processus commerciaux et les questions organisationnelles ». Sur ce constat, ils proposent un cadre global pour évaluer les besoins de l'organisation quant à la SSI.

Pour Solms et al. (1994), la SSI articule plusieurs « facettes » telles que la politique sécurité, l'analyse et la gestion des risques, la planification des ressources et les plans de reprise d'activité. Ils ont alors constitué un modèle sur la base de ces items et proposé une échelle de pilotage de leur mise en œuvre car, selon eux, les top-managers « responsables du bien-être de l'organisation, sont seulement intéressés par le statut actuel de la SSI dans leur organisation. Ils veulent déterminer si leurs services informatiques sont protégés ou non de façon adéquate » (Solms et al. 1994 p. 152 - 153).

Albrechtsen et Hovden (2009 p. 488) justifient le management de la SSI en expliquant qu'un dispositif adressant seulement « des mesures technologiques et de contrôle de ce que les utilisateurs peuvent et ne peuvent pas faire » ne suffit pas alors que « des exigences documentées et des mesures passives de l'information sont basées sur des utilisateurs qui sont supposés raisonnables et se comportant toujours conformément aux exigences de sécurité de l'information et qui acquièrent la connaissance nécessaire en lisant la documentation ».

Straub (1990) a utilisé la théorie de dissuasion générale pour comprendre si la SSI permettait de dissuader les abus sur le SI. Il a conclu que les mesures de sécurité telle que les politiques et des directives d'utilisation appropriée et les pénalités sont efficaces. Il précise que la préoccupation pour la SSI des managers est fonction du niveau de risque perçu. « Une **perception erronée dans ce cas**, cependant, pourrait avoir de **sinistres conséquences** » (Straub 1990 p. 256). Straub et Welke (1988) ont démontré, sur la base de la théorie de dissuasion générale, qu'un programme de sécurité peut être efficace pour contrer les abus en assurant au contrevenant qu'il sera sanctionné. Ils notent que la SSI est ignorée par des directeurs, entrainant des systèmes organisationnels de protection moins efficaces. Selon eux, « le problème sous-jacent est que beaucoup de **directeurs ne sont pas bien informés** de la nature des risques (SI) » (Straub et Welke 1998 p. 442). Goodhue et Straub (1991) ont fait l'hypothèse qu'un individu établit si des mesures de sécurité sont adéquates en fonction (1) du potentiel pour l'abus dans une industrie donnée ; (2) des actions spécifiques prises

pour maintenir la sécurité ; (3) des facteurs individuels comme le degré de connaissance de l'informatique, du rôle managérial, … Particulièrement, Goodhue et Straub (1991) évoquent deux raisons possibles pour lesquelles les mesures de sécurité des organisations financières sont plus développées : 1) les pertes sont potentiellement très conséquentes en cas de violation des SI, 2) une image défavorable véhiculée par la divulgation d'une violation des SI serait critique pour le succès de leurs affaires.

En conclusion, **les facteurs individuels seuls n'influent pas sur le niveau de sécurité perçu** (Goodhue et Straub 1991). Kankanhalli et al. (2003), prolongeant les travaux de Straub et Welke (1998), ont conclu que les top-managers n'investissent pas la SSI. En s'appuyant sur les commentaires de Straub (1990) ils ne s'engageraient pas pour la SSI car ils pensent que : 1) le **risque est faible** ; 2) les bénéfices de la **SSI ne sont pas quantifiables** ; 3) ils **manquent de connaissance** sur les mesures SSI. Hu et al. (2011) ont poursuivi ces travaux et, en indiquant que la dissuasion n'est pas suffisante pour que les règles de sécurité soient respectées, ont constaté que la théorie de choix rationnel peut expliquer **les comportements déviants**. Ils indiquent que « les **avantages perçus** de violations dominent souvent les risques perçus dans le calcul individuel de décision » (Hu et al. 2011 p. 60). Sur la base de la stratégie de l'organisation comme point central de la SSI, Dhillon et Torkzadeh (2006) ont étudié les **valeurs individuelles** pour la protection du SI, révélant 16 objectifs majeurs pour maintenir la SSI dans l'organisation. Loch et al. (1992) ont établi une taxonomie des menaces auxquelles les SI sont exposés. Ils notent que leurs « découvertes révèlent les ironies de sécurité informatique. Les répondants ont semblé avoir **conscience des menaces**, mais voient leur **risque modérément bas** (Loch et al. 1992 p 185).

Pour Eloff et Solms (2000) la SSI a pour objectif premier de protéger le SI et il s'appuie alors sur un cadre permettant d'en définir le fonctionnement attendu. Le cadre proposé vise à articuler le SI et la SSI en définissant des processus à partir des standards et bonnes pratiques. Dans cette veine, il est nécessaire de combiner des mesures de sécurité qui, lorsqu'elles sont mises en œuvre efficacement, permettront de réduire l'impact des risques un niveau minimal acceptable (Hagen et al. 2008 ; Solms 1999). Hagen et al. (2008) s'interrogent justement sur l'efficacité perçue des mesures de sécurité avant de conclure qu'il s'agit principalement d'une association entre le **management des risques** et le développement de la **culture sécurité**. Karyda et al. (2005 p. 247) précise que la SSI « a pour but de minimiser des risques auxquels les SI font face et inclut un certain nombre de phases différentes » : planification, mise en œuvre, évaluation, et formation / éducation. Si la SSI est

complexe par nature, les sociétés disposent de plusieurs cadres « standards » pour gérer les risques SI. Ces cadres suggèrent 1) la nécessité d'acteurs internes « motivés et compétents » pour lier les principes de sécurité à la culture de sécurité ; 2) l''importance du support des top-managers pour la promotion de comportements adéquats et de la culture associée (Kwon et al. 2012).

Knapp et al. (2006) ont défini et testé un modèle pour démontrer l'influence de l'engagement et du support de la direction générale sur la culture de sécurité d'une organisation. L'engagement de la direction générale envers la SSI se démontre par les pratiques qui sont observées par le salarié, acteur individuel (telles que l'organisation de programmes de formation et de sensibilisation). Ainsi des études précédentes ont indiqué le rôle positif de la direction générale et top-managers dans le changement de culture organisationnelle (Knapp et al. 2006). De leur conclusion, nous retenons un verbatim de leurs entretiens : « S'il n'y a aucun support du top management, réel ou perçu, tous les programmes de sécurité de l'information échoueront » (Knapp et al. 2006 p. 32). En outre Kayworth et Whitten (2010) soulignent la faible prise en compte de la stratégie de l'organisation pour la SSI. Ceci a pour conséquence des orientations et des budgets affectés à la SSI qui ne reflètent pas les besoins d'affaires. La pression réglementaire croissante sur la SSI (telle que les lois de notification d'infraction de données d'état aux États-Unis) ne semble pas, selon eux, avoir sensiblement modifié ce constat. En ce sens, Kwon et al. (2012) font état d'une enquête de PWC qui montre que seulement 19% des 834 directeurs interrogés « ont un contrôle effectif et planifient de réduire des risques de sécurité de l'information » (Kwon et al 2012 p. 220). Cependant, ils concluent de leur étude sur l'implication des managers, que la participation d'un top-manager IT dans l'équipe de direction est associée à une plus faible probabilité d'incident de sécurité (Kwon et al. 2012). Hagen et al. (2008 p. 386) classe l'engagement des directeurs et top-managers comme « une des dimensions les plus importantes d'une culture de prévention de perte ». Ils concluent de leur enquête que 60% « estiment que les managers supérieurs sont en réalité engagés dans le travail de sécurité de l'information dans leurs entreprises ». Selon Kwon et al. (2012) organiser la SSI permet aussi une communication facilitée des comportements que les acteurs devraient adopter, indépendamment des fonctions qu'ils occupent.

Plus particulièrement Kwon et al. (2012), soulignant « l'importance du rôle joué par les top-managers sur l'efficacité du management de la sécurité de l'information » ont identifié, que malgré leur responsabilité, la direction générale n'investit pas la SSI. Ils constatent toutefois que cet engagement est comparable à celui pour le SI. Pour ces auteurs, si les équipes de

direction générale jouent un rôle important dans les principes directeurs des SI, ils agissent alors pour contrôler l'impact d'affaires et l'évaluation des avantages soutenus par le SI.

La réduction de risque pesant sur les SI a un impact positif sur le cours de l'action et la position du marché d'entreprises commerciales, si cela est traité comme une question d'affaires (Solms et Solms 2005). Comme la direction générale traite des sujets impactant la stratégie globale d'affaires, les questions de sécurité de l'information devraient aussi être abordées, attendu qu'elles ont les mêmes effets. La SSI, ainsi abordée lors de réunions au plus haut niveau, serait alignée sur la planification d'affaire globale et sur les politiques, ce qui assurerait son efficacité (Kayworth et Whitten 2010). En ce sens, McFadzean et al. (2007) indiquent que l'efficacité de la SSI est en grande partie déterminée par le leadership de la direction générale et des top-managers.

Cependant, ces mêmes auteurs observent un **manque de compréhension des dirigeants quant à l'importance stratégique de la sécurité de l'information**. Leur étude montre que l'engagement des cadres supérieurs avec la sécurité de l'information est dépendant de deux variables clés : 1) **l'importance stratégique de systèmes d'information à leur organisation et** 2) **leur perception de risque** (McFadzean et al. 2007). Ainsi, Goodhue et Straub (1991 p. 14) indiquent que « sans une perte majeure en raison d'une faible sécurité, peut-être que cette préoccupation de sécurité sera généralement tout à fait faible. Il y a la preuve qu'une perte majeure liée à ''l'abus informatique'' peut amorcer ou renforcer la fonction d'administration de sécurité. Les cadres dirigeants, donc, peuvent continuer à être réticents pour accorder le statut et engager des ressources à la fonction de sécurité informatique. »

Pour Kankanhalli et al. (2003 p. 140) « tandis qu'une telle tendance suggérerait la sécurité informatique comme question clé, ceci n'a pas été le cas en pratique. **L'attention pour la sécurité a été basse comparée** à d'autres questions SI ». Ils complètent en précisant qu'une « préoccupation inadéquate pour la sécurité est une évidence qui permet la survenance d'incidents » Selon ces mêmes auteurs, s'appuyant sur les travaux de Straub (1990) qui détaille cette faible préoccupation pour la SSI : 1) les directeurs peuvent prendre une **décision délibérée pour investir peu** dans la sécurité informatique parce qu'ils pensent que le **risque est faible** ; 2) les directeurs peuvent être **sceptiques quant à l'efficacité de la**

SSI informatique en raison de la difficulté d'évaluer les avantages[20] ; 3) les directeurs peuvent **manquer de connaissances** sur les réponses possibles au risque.

Wood (1995 p. 673) remarque que dans le fonctionnement d'une organisation il peut y avoir un « moment favorable » pour initier la SSI, soit « **après que la DG ait perçu l'importance du SI** », soit « après **une infraction majeure** de sécurité des SI, un rapport d'audit informatique défavorable, **un procès** concernant la sécurité, ou un **certain type de pertes** qui a reçu une vaste attention de la direction générale ». Il ajoute, avec une certaine ironie « ceci est un bon temps pour initier les efforts … parce que la direction - à ce moment là - est particulièrement "sponsor" et préoccupée par la sécurité de l'information. Le praticien devrait travailler vite parce que le niveau de préoccupation de la direction diminue très rapidement » (Wood 1995 p. 673).

En synthèse sur la SSI et le management, nous notons que :

1. L'implication de la direction générale et des top-managers est importante car 1) ils disposent de la vision stratégique nécessaire pour définir une SSI efficace (Posthumus et Solms 2004) ; 2) leur participation est requise dans la conception, la mise en œuvre et le maintien de la SSI (Goodhue et Straub 1991 ; McFadzean et al. 2007 ; Straub et Welke 1998) ; 3) ils peuvent influer le changement de culture sécurité (Knapp et al. 2006).
2. Sans une perte majeure en raison d'un faible niveau sécurité, la préoccupation des directions générales peut rester réduite (Goodhue et Straub 1991 ; Hu et al. 2007 ; Wood 1995)
3. Les influences externes et réglementaires n'ont pas systématiquement une influence positive sur la mise en œuvre de la SSI (Kwon et al. 2012)
4. Dlamini et al. (2009 p. 2) font l'hypothèse que « pendant longtemps la plupart des organisations n'ont pas reconnu l'importance de sécuriser » leur SI car la sécurité était considérée « comme un mal nécessaire qui gêne la productivité », les organisations mettraient en œuvre la SSI « simplement parce que toutes les autres le font »
5. Choobineh et Dhillon (2007) et Hagen et al. (2008) soulignent la prédominance technique sur le SI et sur la SSI, qui pourrait alors expliquer 1) la position

[20] Notons que Kwon et Johnson (2014 p. 452) précisent que l'évaluation des apports de la SSI est difficile parce que son succès se mesure justement parce que « rien n'est arrivé »

hiérarchique faible du responsable SSI ; 2) le manque d'investissement sur la SSI à priori ; 3) la direction générale et top-managers ne possèdent pas le langage consacré (spécialisé), ce qui en limite leur compréhension.

Selon la conception du management de la sécurité de l'information de Solms (2006), nous avons abordé dans ces thèmes (« gouvernance » et « management de la SSI »), les deux premières bases qu'ils énoncent pour la sécurité (« l'engagement du board et du top management », et les « structures organisationnelles appropriées ».) Nous pouvons alors traiter ces fondamentaux, dans la déclinaison formelle des principes de sécurité : la politique de sécurité des SI.

2.4.3. Politique de sécurité des SI

Selon Whitman (2004 p. 52), si un professionnel de la sécurité est questionné sur les fondamentaux de la SSI, « il répondra sans hésiter » 1) « protégez votre réseau » et 2) « **rédigez une bonne politique de sécurité ».**

Plusieurs auteurs définissent la PSSI comme permettant d'établir une **infrastructure organisationnelle support**, soit des **orientations** et un **cadre général** précisant le fonctionnement et les responsabilités **en termes de SSI** (Whitman et Mattord 2009 ; Wood 1995). En ce sens, nous retrouvons les éléments structurant du MSSI, tels que décrits dans le thème « Gouvernance ». Ainsi, la stratégie SSI est traduite en orientations dans la politique, définissant elle-même une structure organisationnelle contribuant à l'articulation du contrôle et de la conformité (gouvernance) en synergie avec la façon dont doit être managé la SSI (Posthumus et Solms 2004). La PSSI peut donc être tenue pour la colonne vertébrale du management de la sécurité des SI car elle permet de disposer d'une référence commune à toute l'organisation permettant la compréhension des enjeux, des concepts et des mesures et dont l'ensemble des acteurs doit tenir compte (Höne et Eloff 2002a). Da Veiga et Eloff (2007 p. 363) précisent que « le comportement des employés doit être encadré et surveillé pour assurer la conformité avec les exigences de sécurité et donc de la PSSI ». Cette nécessité de la PSSI est prolongée par Barlette et Fomin (2010 p. 121) qui soulignent l'importance de la définition des responsabilités pour la SSI en indiquant que « sans une politique, les pratiques de sécurité seront développées sans démarcation claire des objectifs et des responsabilités ». Ainsi, les orientations de la sécurité du SI, énoncées par la direction générale (cf. le thème « gouvernance »), se déclinent en principes dans la PSSI (Baskerville et Siponen 2002 ; Solms

et Solms 2006a). En ce sens, Posthumus et Solms (2004) précisent que diriger une organisation nécessite de produire une PSSI qui intègre la direction et le contrôle de la sécurité de l'information.

La littérature est riche de travaux sur les politiques de sécurité, traitant de leur élaboration et adaptation à l'organisation, de leur implémentation et efficacité, ainsi que du respect des règles qu'elles énoncent.

Élaboration et adaptation à l'organisation

En regard de la finalité de la PSSI, « élément structurant de la SSI », il nous apparait important de s'interroger sur la façon dont elle est formulée. Plusieurs auteurs recommandent que la PSSI soit créée à partir des principes fondamentaux de sécurité afin d'assurer qu'ils soient explicitement adaptés aux besoins et circonstances spécifiques de l'organisation dans laquelle elle s'applique (Doherty et Fulford 2006 ; Hagen et al.2008 ; Höne et Eloff 2002). Cependant, Karyda et al. (2005 p. 247) précisent que « la formulation d'une politique de sécurité effective peut être une activité très exigeante et compliquée ». En ce sens, Doherty et al. (2011 p. 208) indiquent que « si elle est créée en coupant et collant simplement des morceaux de la politique pro-forma ou d'autres politiques de l'organisation, il est peu probable que sa formulation ait beaucoup de sens ». Höne et Eloff (2002a) s'interrogent sur la pertinence d'une PSSI dont les principes seraient extraits de PSSI existantes et mises en œuvre dans des organisations comparables. Abrams et Bailey (1995 p. 128) suggèrent que la « politique doit adresser les biens informationnels de l'organisation, les menaces qui pèsent dessus et les mesures décidées par le management ». Ces mêmes auteurs indiquent que, s'il est nécessaire de couvrir tous les risques, une PSSI qui couvrirait « tous les sujets du périmètre (de l'organisation) peut résulter en une politique confuse » (Abrams et Bailey 1995 p. 135). Pour lever les ambiguïtés de la PSSI, ils recommandent d'employer un langage naturel pour formuler des règles compréhensibles et applicables par tous les acteurs afin qu'elle « exprime la politique souhaitée et qu'elle soit correctement utilisée pour mettre en œuvre la SSI » (Abrams et Bailey 1995 p. 132). Pour répondre à cette problématique, Baskerville et Siponen (2002) ont montré l'importance de disposer de politiques dont les principes sont adaptés à chaque activité de l'organisation et proposent un cadre pour leur formulation. En ce sens, Wood (1995) précise que l'analyse de risque est le préalable nécessaire et incontournable pour articuler méthodologiquement et adapter les principes énoncés à l'organisation et ses acteurs. Il précise que le développement d'une PSSI

nécessite de se « référer à l'analyse des risques qui indique clairement les besoins de sécurité » et qu'il s'agit du « point de départ pour établir une infrastructure organisationnelle appropriée, i.e., que c'est l'essence à partir de laquelle les autres éléments de l'infrastructure sont dérivés » (Wood 1995 p. 668). Solms (2000 p. 616) complète ce point en indiquant que « l'analyse de risque est incontournable pour traiter les risques spécifiques qui ne seraient pas adressés dans le guide de bonnes pratiques » (Solms). Enfin Straub et Welke (1998) positionnent l'analyse de risque comme l'outil nécessaire aux managers d'une part pour traiter et comprendre les risques auxquels l'organisation doit faire face et d'autre part pour permettre la mise œuvre de « contre-mesures » adaptées.

Nous avons constaté l'accent mis par plusieurs auteurs quant à l'alignement nécessaire entre SI et SSI, que la PSSI doit justement énoncer. En effet, selon Kwon et al. (2012), la SSI implique des domaines fonctionnels différents dont le bon fonctionnement permet l'atteinte des objectifs d'affaires. Nous avons évoqué, dans le paragraphe « 2.1 Importance des SI » le lien majeur entre SI et « affaire » puis, dans le paragraphe « 2.2 Sécurité du SI » ce qui justifie de protéger le SI. En ce sens, la PSSI doit articuler SI et SSI d'une part et SSI et stratégie d'entreprise d'autre part (Hagen et al. 2008). Ce point est justifié par le constat de Doherty et Fulford (2006 p. 61) : « l'alignement explicite de la PSSI avec le plan des systèmes d'information stratégiques pourrait être une façon constructive de rendre la sécurité de l'information plus pertinente et significative pour les top-managers ».

Devant la complexité d'une PSSI qui satisfasse les exigences des organisations et des utilisateurs, les chercheurs ont étudié l'impact des standards et normes internationales sur l'élaboration des PSSI. Plusieurs auteurs notent que les PSSI sont des exigences essentielles demandées par les standards, normes et guides de « bonnes pratiques » internationaux pour le management de la sécurité des systèmes d'information (Doherty et Fulford 2006 ; Siponen et Iivari 2006 ; Solms 2005). Siponen et Willison (2009) indiquent que souvent, le contenu de la PSSI est issu des standards, normes et « bonnes pratiques », ne faisant que peu de cas des éléments spécifiques à chaque organisation pour la définition des principes qu'elle doit adresser. Pour Höne et Eloff (2002a) et Doherty et Fulford (2006), peu de ces normes et standards décrivent les principes réels de sécurité de l'information à inclure dans la PSSI, c'est à dire les différents thèmes qui devraient être abordés par le document. Dagorn (2012) souligne les difficultés que les organisations rencontrent pour l'emploi des normes et standards par le fait qu'elles sont abstraites et qu'elles ne permettent pas d'aider l'élaboration des PSSI. Pour Baskerville et Siponen (2002) deux points modèrent l'utilisation

systématique des normes et standards : premièrement, une approche standard ne tient pas compte des organisations différentes par nature (et ainsi de leurs différents besoins de sécurité) ; deuxièmement, ils ne tiennent pas compte des incompatibilités qu'il peut y avoir entre les exigences business et sécurité. Dhillon et Backhouse (2001) complètent cette critique en soulignant que les normes et standards ne permettent pas de considérer la nature sociale de l'organisation.

Implémentation et efficacité

Knapp et al. (2009) indiquent qu'un « programme de sécurité » des SI débute avec la politique, dont les instructions écrites sont communiquées à toutes les parties prenantes. En effet, selon ces auteurs, il est nécessaire que les responsables et les utilisateurs s'approprient et mettent en œuvre les principes et règles de la PSSI. Ainsi, Soomro et al. (2016) suggèrent que le rôle des employés soit considéré dans l'implémentation de la PSSI. En effet, si les résultats d'Albrechtsen et Hovden (2009 p. 483) font ressortir l'importance pour les managers « d'informer les acteurs de l'existence d'un système d'exigences quant au comportement d'utilisateur », ils indiquent également que les « managers croient que les utilisateurs ne lisent pas les PSSI » et ainsi « doutent qu'ils aient un effet notable sur la sensibilisation ou le comportement de ceux à qui ils sont destinés ». Cependant, le rôle et l'implication des utilisateurs est central pour la SSI car, comme le précisent plusieurs auteurs, le facteur humain souvent considéré comme le maillon faible de la SSI, peut être une force ou la seule barrière pour prévenir les incidents de sécurité (Albrechtsen 2007 ; Doherty et al. 2011 ; Spears et Barki 2010).

Ainsi, selon Hagen et al. (2008 p. 380), les acteurs de l'organisation peuvent contribuer efficacement à la SSI, si les règles de la SSI énoncées dans la PSSI sont transférées dans la « connaissance tacite et la conscience inconsciente ». Cela repose notamment sur des programmes de sensibilisation « pour accroitre la connaissance des utilisateurs et l'engagement du top management ». Ils appuient leur recommandation sur les résultats de leur étude concluant, qu'une fois que la PSSI est établie, les utilisateurs évaluent la sensibilisation comme la mesure la plus efficace (Hagen et al. 2008).

Knapp et al. (2009) ont défini un méta modèle de PSSI, qui tient compte davantage du contexte de l'entreprise, incluant les influences externes et internes qui peuvent avoir un impact sur les processus organisationnels. Ils indiquent que les organisations sont intéressées par les « méta modèles » de PSSI. Ils suggèrent que cela peut s'expliquer car les

organisations cherchent « des conseils dans le développement et l'amélioration de leurs processus de politique de sécurité … le besoin de tels conseils est clairement prouvé par le fait que quelques organisations n'ont pas de politique de sécurité formelle en place … tandis que d'autres ont des politiques déficientes avec, comme un interviewé l'a exposé, "des formats incohérents et inadaptés, une structure et une couverture des sujets incomplètes, une formulation ambiguë et une faible articulation entre risque et intention" *(de le couvrir)* » (Knapp et al. 2009 p. 502).

Plusieurs études traitant de l'efficacité des PSSI ont été réalisées. Kankanhalli et al. (2003) et Doherty et Fulford (2006) soutiennent qu'une PSSI n'est efficace qu'à la condition d'être supportée par la direction générale et le top management. D'une part, cela converge avec les résultats de Kwon et al. (2012) qui ont montré que la participation du top management était associée à une plus faible probabilité d'incident de sécurité. D'autre part, selon Kayworth et Whitten (2010) et Soomro et al. (2016), si la SSI est organisée au plus haut niveau de l'organisation, elle pourrait être alignée sur la planification des activités globales et les politiques, ce qui assurerait son efficacité. Enfin, la participation des top-managers à la SSI a une influence significative sur l'attitude des salariés et le comportement de conformité aux PSSI (Hu et al. 2012).

Höne et Eloff (2002a) et Whitman (2004), pour qui la PSSI est le moyen formel d'indiquer aux acteurs ce qui est attendu, positionnent la communication de ces règles SSI comme un facteur de succès. Knapp et al. (2006) renforcent ce point en indiquant que l'efficacité de la PSSI est assurée lorsqu'elle est adoptée par des acteurs. Fulford et Doherty (2003) ont réalisé une étude empirique sur les facteurs-clés de succès des PSSI qui a révélé une différence importante entre les principes abordés et des méthodes de diffusion disparates dans chaque organisation. Pour Karyda et al. (2005), les caractéristiques organisationnelles jouent un rôle majeur pour la mise en œuvre réussie et l'adoption de la PSSI. Les critères de succès reposent sur une organisation cohérente dans laquelle les acteurs suivent les codes de la culture sécurité. Particulièrement, Hagen et al. (2008) indiquent que la PSSI est une mesure préventive qui est effective lorsque le reporting des incidents et des infractions est réalisé. Les travaux de Baskerville et al. (2014 p. 149) confirment, dans leur étude sur les incidents de sécurité, l'importance de la PSSI qui « fournit des connaissances et éclairages de la façon dont l'organisation choisit d'équilibrer entre les mesures de prévention et de réponse comme une base actuelle pour sa position vis-à-vis de la sécurité de l'information ».

Si pour Straub (1990) la PSSI adresse les règles d'usages des SI et qu'elle est une condition préalable à la dissuasion, Siponen (2000) puis Albrechtsen (2007) ont montré que, bien que les directives SSI aient une nature normative et impérative pour les acteurs, ils échouent souvent à les appliquer comme prévu. Pour Karyda et al. (2005 p. 247), « bien que la formulation et l'utilisation d'une politique de sécurité soit une pratique commune et que les organisations consacrent des ressources significatives aux activités de management de la sécurité, il est banal que trop souvent l'application d'une politique de sécurité échoue à accomplir ses buts. En conséquence, les directives ne sont pas souvent efficaces s'agissant de leur influence sur le comportement humain et les attitudes. Pour Karyda et al. (2005 p. 147), il y a « une variété de raisons qui ont été avancées pour expliquer le manque d'efficacité dans l'utilisation de PSSI », en effet, selon ces auteurs « les mesures de sécurité que la PSSI définit constituent souvent "une barrière au progrès" et les PSSI vont très probablement être contournées par les acteurs dans leur volonté d'exécuter efficacement leurs tâches ».

May (2003) puis Doherty et Fulford (2006) remarquent que les PSSI sont généralement mises à jour en réponse aux failles de sécurité et/ou à des changements technologiques. Elles ne sont donc **pas conçues comme un cadre de référence préventif** permettant d'assurer que les objectifs de l'organisation soient atteints (Da Veiga et Eloff 2007 ; ISO/IEC 27000 2016). Le manque d'alignement des PSSI avec les objectifs de sécurité est également souligné par Doherty et al. (2011) qui, précisément, soulèvent la question de l'adéquation de l'application des PSSI vis-à-vis des risques encourus par l'organisation. Ce point porte un intérêt particulier sur la connaissance et l'adoption des PSSI par les acteurs. Il renforce les principes énoncés dans la littérature, indiquant qu'une **PSSI doit être définie en regard des risques et non pas élaborée par l'agrégation de règles standards** (Doherty et al. 2011).

Nous retenons du thème « Politique de sécurité des SI » trois points fondamentaux pour le management de la sécurité. Premièrement, Choobineh et Dhillon (2007 p. 958) définissent que le « management de la sécurité des SI est principalement concerné par des questions stratégiques, tactiques et opérationnelles encadrant la planification, l'analyse, la conception, la mise en œuvre et le maintien du programme de sécurité de l'information d'une organisation ». En regard de cette approche de la SSI nous souscrivons à la conclusion d'Eloff et Eloff (2003) qui précisent que la PSSI en est la clé de voute. En effet, ils indiquent que pour « assurer la sécurité de l'information, l'organisation doit mettre en place un cadre de management de la sécurité qui est partie prenante dans la gouvernance et dont les objectifs sont définis en regard de la stratégie de l'organisation ». Deuxièmement, à notre

connaissance, si les travaux que nous avons mobilisés sur la PSSI indiquent qu'elles doivent être alignées sur les SI et les stratégies d'affaires, puisqu'elles prennent en compte les spécificités des organisations, la littérature est silencieuse sur l'application de ces principes d'élaboration, ce qui laisse une teinte prescriptive à ces recommandations. Ce commentaire peut prendre le sens évoqué par Kotulic et Clark (2004), qui, justement, énoncent comment leur étude sur la SSI a échoué à cause de la sensibilité du sujet, sur lequel les organisations ne seraient pas enclines à échanger. Troisièmement, si Wood (1995) précise que formaliser les principes de sécurité ne peut se réaliser correctement que par une analyse de risque dont découlent les mesures permettant la rédaction d'une PSSI (afin de garantir l'adéquation des objectifs de sécurité avec les besoins réels de l'organisation), la littérature ne fait pas consensus sur cette pratique, notamment si l'on considère les travaux de May (2003) et Doherty et Fulford (2006), indiquant un fonctionnement réactif quant à la mise à jour des PSSI après un incident.

Nous avons abordé les trois thèmes qui permettent de structurer la SSI dans l'organisation : gouvernance, management de la politique de sécurité des SI. Toutefois, si le risque est un concept central à notre discipline (Bandyopadhyay et al. 1999 ; Doherty et Fulford 2006 ; Siponen et Oinas-Kukkonen 2007 ; Solms et al 1994 ; Wood 1995), nous soutenons que son étude est majeure pour, justement, définir la structure organisationnelle qui permettra d'y répondre. Cela nécessite alors de s'intéresser à **l'identification**, **l'évaluation et l'estimation du risque**.

2.4.4. Analyse de risque

La définition du management de la SSI, selon Silic et Back (2014 p. 294), renvoie à « la définition de cadres, normes et politiques indiquant quelle stratégie doit être déclinée pour se prémunir des risques possibles ». Ainsi, la mise en œuvre de la SSI articule une activité d'analyse de risques, permettant alors la déclinaison de mesures de sécurité pour protéger le SI (Dhillon et Backhouse 2001 ; Choobineh et al. 2007 ; Ma et al. 2009). Si l'étape d'analyse de risque est un processus de la SSI, il nous apparait incontournable d'exposer son déroulement, ses apports pour la sécurité et pour la gestion des risques. Plus précisément, au regard de notre problématique, nous pouvons nous interroger globalement sur **les raisons à l'appui de la décision de gérer ces risques**, sur les méthodes **permettant justement de « se prémunir des risques possibles »** et sur l'application de ces méthodes.

Concept et apport pour la SSI : la gestion du risque SI

Si Peltier (2004) définit la gestion du risque comme le processus d'identification, d'évaluation de la probabilité de l'occurrence du risque et la définition et la mise en œuvre de mesures pour réduire ce risque à un niveau acceptable, les définitions du « management des risques pour la sécurité de l'information » de la littérature dans le champ des SI peuvent se confondre avec les définitions du « management de la sécurité des systèmes d'information ». Notons ici que la dichotomie entre IT et SI se retrouve dans la littérature pour la gestion des risques. Par exemple, Gerber et Solms (2005) distinguent l'analyse de risque, traitant des biens informationnels support (l'IT), de la gestion des risques, centrée sur les conséquences « métier » supportées par le SI.

Pour Solms et al. (1994), le but est de diminuer la **probabilité** que quelque chose d'indésirable arrive (ou la fréquence avec laquelle elle est prévue arriver) ou la **gravité** des conséquences quand cela arrive « vraiment », ou **les deux**. Ainsi le **risque SI se définit comme une combinaison d'une menace et d'une probabilité de perte** (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Dhillon et Torkzadeh 2006 ; Sjöberg et al. 2004). Dans cette veine, Siponen et Oinas-Kukkonen (2007) indiquent que la gestion du risque est un processus systématique pour faire face aux risques pesant sur le SI, par l'application d'une gamme appropriée de mesures de sécurité physiques, techniques ou opérationnelles, pour protéger des actifs informationnels et atteindre des objectifs stratégiques. En regard de notre problématique, nous observons alors **la SSI comme une activité de gestion du risque**, qui fait interagir analyse de risque et mise en œuvre de mesures de sécurité, afin de minimiser les impacts que ces risques pourraient occasionner (Bandyopadhyay et al 1999 ; Choobineh et Dhillon 2007).

Précisément, l'analyse de risque se décline en quatre étapes indissociables que sont l'identification des **menaces**, l'identification des **ressources critiques** exposées à ces menaces, **l'évaluation des pertes** possibles et **l'estimation de la probabilité** de survenance du risque (Choobineh et Dhillon 2007 ; ISO/CEI 27005 2011 ; Solms 1999, 2000). À l'issue de l'analyse, les risques, considérés selon les besoins de l'organisation (activités majeures et objectifs stratégiques) et selon la fragilité des ressources exposées (menaces et vulnérabilités), sont classés par priorité de façon à déterminer les options de traitement adaptées et proportionnées (Choobineh et Dhillon 2007 ; ISO/CEI 27005 2011).

Le croisement de l'évaluation des pertes et de l'estimation de probabilité de survenance des risques est utilisé pour déterminer les dégâts potentiels sur une ressource et les conséquences pour l'organisation (Gordon et Loeb 2002). Particulièrement, Abrams et Bailey

(1995) et Wood (1995) introduisent l'analyse des coûts et bénéfices des mesures de sécurité dans la décision des top-managers. Comparable à la méthode d'analyse de risque que nous avons développée, ces auteurs concluent que l'investissement pour les mesures est mis en perspective des pertes potentielles pour l'organisation. Pour Straub et Welke (1998), la question coût / bénéfices des mesures de sécurité est majeure pour les directeurs. Ils indiquent que cette question est arbitrée globalement en tenant compte 1) des risques inhérents au domaine d'activité de l'organisation, 2) des efforts déjà engagés pour contrôler ces risques et 3) des facteurs individuels (tels que la conscience d'incidents précédents). En ce sens Willison et Backhouse (2006) montrent que la principale raison des faiblesses des dispositifs de sécurité des organisations est leur défaillance à apprécier la valeur des ressources de leur SI et les menaces auxquelles elles sont exposées. Ils précisent alors l'importance de la participation des top-managers à l'analyse de risque pour observer les ressources SI majeures et les menaces potentielles. Ils notent comment les « perceptions éclairées » sont basées sur **la connaissance de trois domaines** : 1) l'environnement organisationnel (la connaissance des risques inhérents à une industrie spécifique), 2) l'environnement du SI (la **connaissance** de la gamme de **contrôles techniques et managériaux** qui peuvent couvrir le risque SI) et 3) les **caractéristiques individuelles** (la connaissance propre des risques potentiels) (Willison et Backhouse 2006 p. 403-404). Pour ces mêmes auteurs, il est nécessaire d'accompagner les top-managers dans l'identification de ces éléments pour analyser les risques convenablement.

Plusieurs auteurs appuient l'importance d'une analyse centrée sur les dysfonctionnements des SI qui impacterait l'activité de l'organisation, pour permettre la définition d'un niveau de sécurité adapté (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Choobineh et al. 2007 ; Siponen et Oinas-Kukkonen 2007). Ce point fait consensus dans la littérature, pour exemple Choobineh et Dhillon (2007) mentionnent que les **ressources du SI** peuvent être analysées et classées selon **leur valeur** en considérant la façon dont **elles soutiennent les objectifs stratégiques de l'organisation.** En effet, les réponses à mettre en œuvre pour couvrir les risques (mesures de sécurité), nécessitent de prendre en compte la stratégie de l'organisation, ses spécificités et le contexte dans lequel elle opère (Backhouse et Dhillon 1996 ; ISO/CEI 27005 2011). Ainsi, selon Bandyopadhyay et al. (1999), en regard de la position centrale du SI dans l'organisation, seule une vue holistique considérant le **spectre entier de l'environnement de l'organisation**, au-delà du seul SI, permet d'évaluer les potentiels risques. Cette approche souligne que l'analyse de risque n'est pas un simple calcul de probabilité d'impact mais plutôt que l'identification des risques et la protection des

risques sont particuliers à chaque organisation impliquant d'observer les impacts pour l'organisation et ses spécificités.

Nous pouvons synthétiser le besoin de connaitre les risques en citant un commentaire de Posthumus et Solms (2004 p. 640), qui, de notre point de vue, mérite une attention particulière : « afin de protéger les informations sensibles de l'entreprise à partir des différents risques qui peuvent avoir une incidence, il est important de **comprendre exactement de quelles sources ces risques** peuvent survenir ». En effet, l'analyse de risque est un processus de décision qui permet la compréhension des risques qui s'imposent au SI et la définition des réponses. D'un autre point de vue, les incidents de sécurité SI peuvent se mettre en perspective de la valeur et l'importance qu'accorde une organisation à ses ressources informationnelles, de par les conséquences dommageables que ces risques auraient pour l'organisation. Ainsi pour Posthumus et Solms (2004), protéger les SI de l'organisation à partir des différents risques pouvant les affecter est une tâche difficile en regard de la nature et la diversité des risques qui s'imposent. Notamment, les organisations doivent faire face à trois sources de risques (Loch et al. 1992 ; Posthumus et Solms 2004) : 1) les phénomènes naturels (inondations, tremblement de terre, foudre, feux…) ; 2) les risques techniques (bug ou dysfonctionnements tels que la transmission de virus ou l'obtention illégitime d'accès) ; 3) les risques humains (actes délibérés ou accidentels). Posthumus et Solms (2004 p. 641) ajoutent que « chacune de ces diverses sources de risques dans les organisations présente un véritable défi quand il s'agit de fournir une protection adéquate de leurs ressources d'information » et « il est très important que chacune de ces sources de risques soit traitée afin d'assurer la confidentialité, l'intégrité et la disponibilité des informations de l'entreprise, tant du point de vue interne qu'externe ». Cela rejoint la définition de l'objectif de la gestion des risques de Bandyopadhyay et al. (1999 p. 437) qui est de « protéger des actifs informationnels comme des données, le matériel, le logiciel, le personnel et des installations de toutes menaces externes (par exemple des catastrophes naturelles) et internes (par exemple des problèmes techniques, du sabotage, des accès non autorisé) pour que les coûts des pertes résultantes de la réalisation de telles menaces soient minimisés ».

Straub et Welke (1998 p. 445) inscrivent l'analyse de risque comme un mécanisme de décision permettant de juger quelles actions seraient pertinentes pour assurer la protection du SI (notons qu'ils appuient leurs propos sur les travaux de Simon précisant que « **les problèmes doivent être identifiés pour pouvoir être résolus** »). Ainsi, afin de guider la réflexion et disposer d'une compréhension plus profonde et globale de gestion des risques SI,

Straub et Welke (1998) ont proposé un modèle fondé sur les travaux de Baskerville (1993). En effet, cet auteur a démontré les limites des méthodes d'analyse de risque employées jusqu'alors, notamment par leur manque de considération des activités de l'organisation car principalement centrées sur les mesures de protection technique des SI. Le modèle de Straub et Welke (1998 p. 449) situe l'analyse de risque dans sa position logique, offrant un « pont entre la formulation de problème et la génération d'alternatives et précédant la phase de décision de planification ». Le mécanisme de décision relève alors de responsables qui disposeraient d'une vision d'ensemble de la stratégie et des activités majeures de l'organisation d'une part, et des risques pesant sur le SI qui supportent ces activités d'autre part.



Figure 6 : Modèle de planification pour traiter les risques SI
(adapté de Straub et Welke 1998)

Les pratiques empiriques étudiées dans la littérature : plusieurs lacunes

S'il fait consensus de la nécessité d'analyser les risques selon une approche holistique de l'organisation et de ses activités, la littérature comporte plusieurs critiques à l'endroit des pratiques empiriques observées.

La pratique **de méthode inadaptée** est pointée par Baskerville (1993) et Dhillon et Backhouse (2001), critiquant l'usage historique des « listes de contrôle ». Selon eux, le concept de cette méthode repose sur le choix des mesures de sécurité qui pourraient être mises en œuvre, plutôt que de s'interroger sur les réels risques à couvrir. Dhillon et Backhouse (2001 p. 137) soulignent ce propos et indiquent une « tradition fonctionnaliste », ayant tendance à se concentrer sur les moyens et **non sur les fins**. Orienté sur la finalité de l'analyse de risque, Siponen (2005) a comparé les principes et les caractéristiques de 17 méthodes d'analyse de risque. Il conclut que la majeure partie des méthodes traditionnelles entraîne une vision technique du rôle organisationnel de la SSI et donc l'importance de la

nature **socio-organisationnelle n'est pas assez sérieusement considérée** (Siponen 2005). En effet, selon lui, la majeure partie des méthodes traditionnelles est basée sur le développement conceptuel, offrant peu d'éclairage sur leur facilité d'utilisation, pertinence en pratique et adaptation à la mise en œuvre de la SSI.

Précisément, ne pas employer de méthode adaptée pour analyser les risques pourrait conduire à une **sécurité réactive** pour **deux principales raisons** (Doherty et Fulford 2006 ; McFadzean et al. 2007) : limiter l'étude aux **aspects technologiques** des SI, ne pas étudier **les risques en regard des activités majeures** de l'organisation.

Attendu que la SSI est souvent perçue comme une **préoccupation purement technique** (Dhillon et Backhouse 2001 ; Solms 2001 ; Soomro et al. 2016 ; Siponen et al 2014 ; Wood 1995) l'analyse des risques est réalisée selon une approche centrée sur les ressources technologiques. Le biais principal de ce type de méthode est qu'elle ne satisfait pas l'étude de la problématique exhaustive et, par conséquent, limite l'appréciation des **éléments qui constituent** le SI et son environnement. En effet, ne pas considérer la dimension socio-organisationnelle des risques écarterait l'étude des changements qui sont inhérents aux organisations tels le contexte, les technologies et les pratiques (Choobineh et Dhillon 2007 ; Dhillon et Backhouse 2001 ; McFadzean et al. 2007). Une approche consistant à choisir des réponses à des problèmes sans les avoir analysés globalement dans leur contexte est antagoniste au modèle de Straub et Welke (1998) **car elle limite, par construction, la pertinence de l'analyse et par conséquence l'éventualité des risques**. Précisément, les défaillances d'une telle approche sont pointées notamment par Solms (2000) et Siponen et Willison (2009). Pour Solms (2000) répondre au risque en employant des standards et guides de bonnes pratiques est insuffisant, car ils ne permettent pas justement de traiter les risques spécifiques à l'organisation. Siponen et Willison (2009 p. 268) confirment ce propos en précisant que les mesures de sécurité génériques peuvent omettre des exigences spécifiques, aboutissant potentiellement à des investissements inopportuns, conduisant à des pertes sur des SI potentiellement « non sûrs ».

Willison et Backhouse (2006) appuient ce constat en précisant qu'une telle approche aboutirait à des mesures de sécurité ne répondant qu'à des risques mineurs laissant ainsi des **activités majeures particulièrement exposées à la survenance d'un** risque. Ils concluent qu'en conséquence les top-managers auraient une représentation « déformée » de la sécurité, conduisant à une compréhension limitée des risques à couvrir (Willison et Backhouse 2006). Cette faiblesse à considérer le SI dans son contexte et selon ses apports

majeurs pour l'organisation peut laisser penser aux top-managers que le niveau de sécurité est adapté et ainsi **refléter une réalité biaisée** (Dhillon et Backhouse 2001).

Les apports d'une approche de la SSI en considérant les **activités majeures de l'organisation** sont démontrés par plusieurs auteurs (Choobineh et Dhillon 2007 ; Dlamini et al. 2009 ; Hagen et al. 2008 ; Hu et al. 2007). Cependant, Willison et Backhouse (2006) expliquent le manque d'efficacité de la SSI par la difficulté des top-managers à identifier les mesures adaptées et cohérentes. Ils pointent une articulation non systématiquement établie entre fonctions métiers et sécurité, conduisant à mettre en place des mesures inopportunes ou inefficaces, et créant alors une fausse impression de sécurité (Willison et Backhouse 2006). Ce commentaire peut être prolongé par celui de Spears et Barki (2010) qui considèrent que les acteurs de l'organisation peuvent être une partie de la solution en positionnant davantage les efforts pour la SSI sur la participation des responsables métier de l'organisation que sur la seule protection des actifs technologiques. Loch et al. (1992) ont classé les risques SSI perçus par les tops-managers ayant des fonctions dans le champ des SI. Ils précisent que « **le niveau des risques perçus est plus bas que ce qu'il ne devrait être** » (Loch et al. 1992 p. 185), et en cela rejoignent les constats de Straub (1990). Ils soulignent que la faible implication des top-managers peut avoir pour conséquence une estimation non réaliste des potentiels risques inhérents au SI dans un environnement interconnecté. Selon Kotulik et Clark (2004), les organisations doivent rencontrer un incident impactant leur activité pour que les menaces et vulnérabilités des SI supports soient considérées, expliquant alors **l'approche réactive pour la SSI**.

Plusieurs travaux convergent pour expliquer les lacunes des méthodes d'analyse de risque, aboutissant à des mesures de sécurité inadaptées (Doherty et al. 2011 ; Gordon et Loeb 2002 ; Siponen 2005 ; Siponen et Willison 2009 ; Solms 2000). Nous retenons de ces études académiques la faiblesse des méthodes d'analyse de risque quant à la mise en œuvre de mesures répondant au **besoin de sécurité des ressources SI majeures** (Gordon et Loeb 2002), notamment par **l'absence d'étude systématique des risques** (Willison et Backhouse 2006).

Gestion des risques : décision et responsabilités pour la SSI

La SSI adresse prioritairement les questions stratégiques, tactiques et opérationnelles définissant la planification, l'analyse, la conception et la mise en œuvre de la protection globale des activités de l'organisation dont le SI est support. Si Choobineh et Dhillon (2007)

confirment l'importance des décisions relatives à la gestion des risques pour le bon fonctionnement des SI des firmes et leurs activités, ils notent que la complexité de l'organisation et ses interdépendances avec son environnement accroissent la difficulté d'estimer la valeur des ressources organisationnelles critiques et donc les impacts de la survenance d'un risque. Ce constat peut être mis en perspective des travaux de Tsohou et al. (2006 p. 199) précisant justement « qu'aucune solution de sécurité n'est appropriée pour toutes les organisations ». Tsohou et al. (2006) indiquent que beaucoup d'organisations traitent le risque selon la **perception de leurs top-managers et leur attitude envers ces risques**. Ils précisent que souvent, la gestion des risques est basée sur la perception des risques associés aux ressources IT (Tsohou et al. 2006). Ainsi, le problème majeur auquel doivent répondre les top-managers en termes de gestion des risques, est que le risque lui-même est un **concept abstrait** (Gerber et Solms 2005 ; Tsohou et al 2006). En effet, le risque est une combinaison complexe de facteurs qui doivent être considérés selon un jugement humain lors de l'analyse (Tsohou et al 2006).

Plusieurs auteurs pointent le faible intérêt des directions générales pour la sécurité de l'information (Choobineh et al. 2007 ; Loch et al. 1992 ; Straub 1990 ; Straub et Welke 1998). Nous nous intéressons particulièrement au modèle de gestion des risques développés par Straub et Welke (1998), dont la première étape consiste justement à **identifier le risque SI**. Pour ces mêmes auteurs, le risque peut être géré quand les directeurs sont informés de la gamme complète des mesures disponibles et qu'ils mettent en œuvre les mesures les plus effectives. Cependant, nous comprenons qu'il soit nécessaire de définir les seules mesures cohérentes avec les activités à protéger prioritairement (Peltier 2004). Il ne semble pas fondé de définir « ex nihilo » des mesures dont on n'aurait pas perçu la pertinence mais qui aurait été **déployées par mimétisme**. Pour cela, « l'analyse de risque assurera que toutes les décisions sont basées sur les besoins de l'entreprise et que les mesures prudentes et raisonnables sont mises en œuvre » (Peltier 2004 p. 48).

À notre connaissance, aucune étude académique ne traite de la conscience des risques SI des top-managers et des réponses à y apporter. Toutefois, deux études ont eu pour objet l'approche des organisations quant à l'analyse de risque.

Tsohou et al. (2006) ont établi, sur la base des travaux de la théorie culturelle de Douglas (1978) et Douglas et Wildavsky (1983) une articulation théorique entre type de **biais**

culturels[21], **perception des risques** et **méthode d'analyse de risque** SI. Ils identifient les facteurs sociaux tels que la perception des risques comme déterminants pour l'approche des risques et le contexte social dans lequel sont établies les mesures de sécurité. Selon eux, sur la base des **biais culturels** (hiérarchiste, égalitariste, individualiste, fataliste) les méthodes d'analyse de risque et les mesures de sécurité mises en œuvre sont différentes (Tsohou et al. 2006). Ces travaux s'inscrivent dans notre perspective de recherche. En effet, ils renforcent le concept qui vise à établir un lien entre les décisions quant à la **prise en compte et au traitement du risque SI selon les caractéristiques individuelles des décideurs**.

McFadzean et al. (2007) ont identifié un lien entre **contexte institutionnel**, **risques perçus** par les top-managers, **importance accordée au SI** et **stratégie visée** par les organisations. Selon eux, la perception des risques par les managers a un rôle sur leur investissement pour la SSI. En ce sens Hagen et al. (2008 p. 384) confirment l'importance du **contexte institutionnel** en soulignant que « l'analyse de risque, les audits internes et les audits externes sont significativement plus répandus dans l'activité financière que dans les autres secteurs ». Précisément, la **perception des risques des directeurs** influencera leurs rôles et les décisions institutionnelles telles que les considérations budgétaires ou réglementaires pour la SSI. Autrement dit, une entreprise dont le SI est utilisé comme « une arme compétitive dans un environnement à haut risque », investira plus la SSI qu'une entreprise utilisant son SI comme « une nécessité opérationnelle dans un environnement de risque faible » (McFadzean et al. 2007 p. 635). Bien que la perception des risques soit mobilisée dans leur étude, aucun éclairage n'est porté sur les facteurs sur lesquels est basée leur perception.

Nous nous intéressons particulièrement à la façon dont **sont objectivées ces menaces et ces pertes potentielles**. Plus précisément, nous observons ces risques en regard de l'impact perçu qu'ils auraient **sur l'organisation** en cas de survenance sur le SI. En accord avec la problématique que nous développons, **nous considérons ces risques selon le point de vue des décideurs**, notamment ceux pour qui « les risques auraient des implications sérieuses » (selon Moulton et Coles 2003 p. 580). Notons qu'Abrams et Bailey (1995 p. 127) soulignent que parfois les managers prennent les décisions de couverture des risques 1) sans qu'une analyse de ces coûts et bénéfices ne soit possible (risques et mesures), 2) « **sur la base d'informations insuffisantes** fournies par leurs subordonnés ». Ceci renforce notre

[21] La théorie culturelle des risques développée par Douglas permet de fournir de explications sur comment et pourquoi les individus formulent leur perception des risques et des menaces.

interrogation sur l'articulation risque / besoins majeurs de l'organisation (telle que développée notamment par Hagen et al. 2008) et sur le rôle majeur des top-managers quant à la définition des orientations et principes de sécurité. Rappelons que selon Hu et al. (2007) si la décision de gérer les risques SI ne provient pas du plus haut de l'organisation, la nécessité de protéger le SI peut être remise en cause et manquer d'efficience. Ainsi, si la décision de gérer les risques est basée sur des informations parcellaires nous pouvons prolonger cette réflexion et nous interroger plus globalement sur quels risques sont effectivement considérés.

Selon la littérature, la SSI a pour étape fondamentale l'analyse de risque, permettant d'objectiver les menaces, risques et conséquences. Elle offre une approche méthodique aux décideurs pour mettre en place les mesures de sécurité adéquates afin de se prémunir des risques. Si l'analyse de risque est réalisée lors de la mise en œuvre de la SSI, nous pouvons nous interroger sur les risques **qui sont à l'origine de l'initiation de la SSI**. Il s'agit alors d'étudier les risques pris en compte lors de la décision de mettre en place la SSI.

Un thème émergeant de la littérature et traitant justement d'une raison possible pour la mise en œuvre de la SSI, outre les risques, relève du respect de la conformité. En effet, selon plusieurs auteurs, la conformité aux lois aux règlements ou aux standards semble être un levier important pour initier la SSI, indépendamment des risques (Hagen et al. 2008 ; Peltier 2004 ; Solms 2006 ; Williams et al. 2009).

2.4.5. Conformité

La conformité dans le domaine de la SSI est étudiée selon trois applications : la **conformité des acteurs** aux règles de sécurité, la conformité aux standards, normes et bonnes pratiques, et la **conformité réglementaire** ou législative qui relève d'une fonction de gouvernance telle que nous l'avons développée dans le paragraphe « 1.1.3 Le management de la sécurité de l'information ». Nous rappelons, en préambule de cette section, que Solms et Solms (2006 p. 410) abordent la conformité comme un **facteur externe** à l'entreprise qu'il convient d'étudier pour les décisions de « gouvernance ».

Conformité aux règles SSI

La **conformité des acteurs aux règles** de sécurité a fait l'objet de plusieurs recherches visant à examiner les comportements relatifs à la protection du SI, selon une perspective criminelle (Straub et Nance 1990 : Straub et Welke 1998 ; Willison 2006 ; Willison et Backhouse 2006), selon une perspective d'adoption des règles (Albrechtsen 2007 ; Bulgurcu, Cavusoglu et Benbasat 2010 ; D'Arcy et al. 2009 ; Herath et Rao 2009b ; Solms et Solms 2004a ; Straub 1990 ; Siponen et Vance 2010 ; Puhakainen et Siponen 2010) ou encore selon **la crainte suscitée par le non-respect** (Boss et al. 2009 ; Ifinedo 2012 ; Johnston et Warkentin 2010 ; Liang et Xue 2009). En effet, selon Soomro et al. (2016), la conformité des acteurs finaux à l'ensemble des règles édictées dans leur organisation aura un impact positif significatif sur la SSI.

Les travaux sur la **conformité de la SSI aux standards, normes et bonnes pratiques** traitent pour certains de leur application et adaptation à l'organisation (Höne et Eloff 2002b) et d'autres de leur importance pour le management de la SSI (Solms 1999). Notons que ces études ne considèrent pas l'aspect obligatoire des standards, normes et bonnes pratiques mais visent à éclairer les pratiques des organisations et l'importance accordée pour la SSI. Ainsi Höne et Eloff (2002b) indiquent que si la **difficulté d'appréhender la SSI** peut être contournée par l'emploi des standards, ceux-ci sont **génériques et prescriptifs**. En effet les standards décrivent les processus et les mesures de sécurité nécessaires pour la SSI plutôt que d'aider à la mise en œuvre globale d'un système assurant la sécurité de l'information (Höne et Eloff 2002b). Ce commentaire est complété par Karyda et al. (2005) qui soulignent deux conséquences défavorables possibles au manque d'adaptation, liées à l'objectif même visé par la « standardisation ». D'une part les mesures non adaptées sont susceptibles d'être contournées par les acteurs car jugées comme un frein à l'exécution de leurs tâches quotidiennes (Karyda et al. 2005). D'autre part, les standards ne permettent pas de satisfaire aux exigences de sécurité particulières et aux objectifs spécifiques à l'organisation et à son environnement (Baskerville et Siponen 2002 ; Karyda et al. 2005). Plus précisément, si les mesures de sécurité pour des « objets technologiques » tels que des serveurs de fichiers ou des équipements réseaux peuvent être semblables dans des organisations différentes, une solution managériale unique ne peut correspondre à toutes les organisations (Karyda et al. 2005 ; Posthumus et Solms 2004 ; Tsohou et al. 2006). Pour Solms (2005), les standards offrent un cadre permettant d'évaluer la conformité de la sécurité de l'information en regard des pratiques normalisés. Cependant, Barlette et Fomin (2010) portent un éclairage particulier sur l'adoption des standards SSI. Ils indiquent qu'un manque **d'implication des**

top-managers, dû à une **faible perception des risques** assortie d'une difficulté à en évaluer les apports peuvent expliquer la faible adoption des standards. Une explication complémentaire peut provenir de Siponen et Willison (2009) qui ont étudié le rôle majeur des standards dans la certification des SI des organisations. Ils ont constaté que les standards étaient universels et génériques, avec pour conséquence de ne pas suffisamment prendre en compte les **différences entre les organisations** et les **différentes exigences de sécurité** qu'elles auraient. Ils ont noté que ces standards ont été validés par l'appel des praticiens et des autorités, critiquant alors leur portée coercitive. Ils ajoutent que les standards doivent plutôt être considérés comme une aide pour le management de la sécurité de l'information à destination des praticiens. Doherty et Fulford (2006) ont une position sensiblement différente. Ils précisent que les standards n'offrent aucun conseil explicite sur la façon de développer la SSI et comment elle pourrait être alignée sur les objectifs de l'entreprise. Ils soulignent que les normes semblent seulement mettre l'accent sur une forme réactive de l'examen de la SSI (par exemple lors de changements technologiques) et n'offrent pas de conseils explicites sur la façon dont justement la SSI pourrait être mieux articulée avec les objectifs organisationnels (Doherty et Fulford 2006). Enfin, Kwon et Johnson (2014) adressent une critique intéressante à l'endroit des standards SSI. Ils précisent que si le débat d'experts sur l'efficacité des réglementations n'est pas tranché, les **directives qu'elles imposent** seraient « contre-productive parce qu'elles poussent à atteindre un certain niveau de mesures, **indépendamment des spécificités** et de la maturité de l'organisation quant aux SI et SSI. Cela conduirait alors à créer une culture de conformité plutôt qu'une culture de SSI. » (Kwon et Johnson 2014 p. 455).

Conformité réglementaire et légale

Attendu l'objet de notre recherche, positionné en amont du processus de sensibilisation et de contrôle des règles et mesures de sécurité, nous poursuivons l'analyse de la littérature sur le thème de la conformité en ciblant davantage de quelle façon les standards peuvent éclairer la décision d'initialiser la SSI. En effet, nous nous intéressons à la phase d'initiation de la SSI, lorsque celui-ci se résume à son adoption symbolique. Ainsi, Pour Silic et Back (2014) la **conformité vise principalement à respecter**, pour l'organisation, **les exigences réglementaires et légales**. En ce sens, la conformité réglementaire et légale des SI est une responsabilité de gouvernance car les conséquences en cas de non-respect peuvent être importantes pour l'organisation (Knapp et al. 2009 ; Moulton et Coles 2003). C'est selon ce

point de vue que nous observons la conformité, comme une **influence externe qui provoquerait la décision** d'adopter symboliquement la SSI.

Mcfadzean et al. (2007) révèlent plusieurs facteurs contextuels pouvant influencer la direction générale quant au développement de la SSI. Parmi les facteurs internes tels que la culture organisationnelle et les facteurs externes tels les menaces, la **conformité aux lois** est considérée comme **un levier majeur** pour la gouvernance. La conformité a ainsi une **influence directe sur les risques perçus** par les top-managers, d'une part car il est obligatoire de s'y conformer sous peine d'astreintes financières ou d'éventuelles conséquences juridiques, et d'autre part car les mesures qu'elle impose peuvent permettre **une prise de conscience des risques** jusqu'alors encourus et sous-estimés voire non considérés. Hu et al. (2007) ont étudié l'impact d'une loi et proposé une explication de l'amélioration de la SSI selon la théorie néo-institutionnelle (Meyer et Rowan1977 ; DiMaggio et Powell 1983). Plus précisément, ils détaillent les influences internes et externes à l'organisation dans le cadre d'une organisation qui devait se conformer à la réglementation « Sarbanes-Oxley » (SOX). Ils ont conclu que les efforts nécessaires à la mise en œuvre du dispositif SSI ont été ré-institutionnalisés grâce à une influence isomorphique coercitive (régulation) sur les tops-managers, une influence normative (groupes spécialisés avec lesquels l'organisation a échangé sur SOX) et mimétiques (les réseaux de connaissances des top-managers en charge du projet de conformité) (Hu et al. 2007). Nous pouvons illustrer la prise de conscience de l'importance accordée à SOX en citant un des top-managers interviewé par Hu et al. (2007 p. 162) : « Sarbanes-Oxley est arrivé et cela a allumé un feu » ce qui indique des efforts déployés conséquents et une nouvelle organisation adoptée pour la mise en conformité. Selon ces auteurs, si les jeux d'influences montantes et descendantes dans l'organisation ont permis le succès du projet, celui-ci repose davantage sur le soutien d'initiatives et la diffusion de la culture à tous les niveaux par les top-managers (Hu et al. 2007).

Particulièrement à la sécurité des SI dans le domaine de la santé, Kwon et Johnson (2014) notent que la dernière décennie a été riche de lois, imposant notamment la communication des incidents de sécurité (aux autorités de tutelles). Ainsi, pour des organismes médicaux, la sensibilité du public à la divulgation de donnés médicales privées provoque « souvent des réactions exceptionnellement fortes à cause de la nature de l'information » (Kwon et Johnson 2014 p. 455). Ainsi, la loi créée une pression double, obligeant la déclaration des incidents et exposant l'organisme médical à une potentielle perte d'image auprès des patients.

Dans une discipline différente de la SSI, Williams et al. (2009) ont étudié la **sécurité des chaines d'approvisionnement** et les régulations qui ont été imposées à leurs prestataires après les attentats du 11 septembre 2001 aux États Unis. Ils précisent que les organisations ont eu comme moteurs, pour la stratégie de sécurisation de leurs chaines d'approvisionnement, les **exigences du législateur et des clients** (isomorphisme coercitif), **les adaptations de la concurrenc**e (isomorphisme mimétique) et les **attentes de la société** (au sens de la Nation, pression normative). Ces influences seront développées au chapitre consacré à l'isomorphisme mais nous pouvons toutefois indiquer comment elles se sont traduites dans l'étude de Williams et al. (2009). L'isomorphisme coercitif est provoqué par le législateur et l'autorité du domaine d'activité, qui imposent la protection des chaines d'approvisionnement contre les atteintes liées au terrorisme ou à la contrebande. Il provient également des entreprises clientes de ces chaines d'approvisionnement. En effet, informées des risques, elles ont alors exigé de leurs fournisseurs la mise en œuvre des mesures recommandées par la réglementation. L'isomorphisme mimétique est déclenché par les changements de fonctionnement des concurrents, qui ont adapté la sécurité de leurs chaines d'approvisionnement. Ainsi, devant la nécessité d'implémenter ces mesures et sous la pression des clients qui le demandaient, les fournisseurs ont mis en œuvre les mesures exigées. Williams et al. (2009) indiquent également à l'appui des travaux de Scott (1995), que les organisations se conforment aux règles à cause des pressions environnementales telles que les **obligations morales et éthiques que leur environnement attend de ces organisations** (Williams et al. 2009). En ce sens, notons l'importance accordée à la conformité à la loi sur la sécurité des chaines d'approvisionnement, soulignée par un des répondants de l'étude de Williams et al. (2009 p. 606) : « Aucune société ne veut être celle qui est responsable de favoriser les actes de terrorisme ». Enfin, ils précisent que les raisons sous-jacentes à ces changements ont été comprises par les top-managers qui ont pu alors allouer les fonds nécessaires à la mise en œuvre d'une sécurité adaptée.

Normes, standards et risques

Nous avons détaillé les raisons pour lesquelles la conformité aux règlements ou aux standards, qui s'imposent aux organisations, relèvent d'une responsabilité de direction générale. Ne pas considérer et appliquer ces exigences peut conduire les organisations à des pertes de marché (Williams et al. 2009) des pertes financières ou d'image (Kwon et Johnson 2014), à des implications juridiques (Höne et Eloff 2002b ; Knapp et al. 2009) ou encore des conséquences directes sur les directeurs et top-managers (Moulton et Coles 2003). À

l'inverse, la prise en compte de ces exigences par les organisations a pour conséquence d'informer les top-managers sur les risques encourus (Williams et al. 2009) et une refonte du dispositif de sécurité des organisations (Hu et al. 2007). Cela rejoint le commentaire de Posthumus et Solms (2004) qui soulignent justement la nécessité de **connaitre les risques**, pour éventuellement mettre en œuvre les mesures pour y répondre. Ainsi, nous retenons de la thématique « la conformité » dans la littérature de la SSI (et plus globalement la littérature sur la sécurité de la logistique en regard des travaux de Williams et al. 2009), la **possible prise de conscience des risques** ou la mise en œuvre de mesures de sécurité exigées par les règlementations ou standards, qui peuvent alors influencer la décision d'adoption symbolique de la SSI.

L'approche normative ou coercitive de la SSI telle que décrite dans la littérature, conduisant ou imposant les organisations à l'adoption de standards peut nous éclairer sur la faiblesse des dispositifs SSI mis en place (Kwon et Johnson 2014). En effet, si l'application des standards peut accompagner l'élaboration du dispositif de sécurité, cela peut conduire à des biais d'efficacité des mesures par manque d'adaptation à l'organisation, à ses spécificités et à ses acteurs (Kwon et Johnson 2014). La littérature traitant des normes, standards et bonnes pratiques fait consensus sur l'analyse de risque comme préalable nécessaire et incontournable pour articuler méthodologiquement et adapter les principes de sécurité à l'organisation et à ses acteurs (Höne and Eloff 2002b ; Solms 2000 ; Straub et Welke 1998 ; Wood 1995). Alors, si les standards appellent les organisations à conduire une analyse de risque préalable à l'élaboration d'un dispositif SSI, nous pouvons nous interroger sur la décision relative à la SSI pour les organisations **auxquelles les standards ne sont pas imposés**. Selon l'approche de Straub et Welke (1998) l'analyse de risque permettrait d'élaborer les réponses aux (seuls) risques qui s'imposent à l'organisation, ces réponses pouvant alors être mises en œuvre effectivement grâce à l'apport des standards.

Les principaux thèmes de recherche en SSI montrent, pour différentes raisons non exclusives, l'importance et la nécessité d'engager la protection des SI. En effet, nous avons démontré l'importance de l'implication des dirigeants pour la SSI, par la responsabilité de protéger le SI de leur organisation (McFadzean et al. 2007 ; Straub et Welke 1998), par leur capacité à définir les orientations stratégiques et de par leur connaissance des enjeux et risques auxquels leur société est exposée. Si la conformité évoquée dans la littérature peut offrir des pistes pour éclairer l'adoption de la SSI, l'analyse de risque est au cœur de la discipline. Précisément, l'étude de ce thème met en évidence la faiblesse de l'analyse de

risques et les conséquences défavorables possibles sur l'efficacité de la SSI. Au cœur de la gestion des risques, les top-managers ont un rôle majeur de par leur connaissance des activités sensibles de l'organisation et par leur capacité à identifier globalement les risques pour y répondre.

2.5. Prolongements théoriques de la recherche en SSI

Crossler et al. (2013), à propos de l'évolution de la recherche en SSI, soulignent les nombreuses publications sur les comportements tels que par exemple la conformité aux politiques (Bulgurcu et al. 2010 ; Herath et Rao 2009a; Hu et al. 2012 ; Siponen et Vance 2010 ; Warkentin et Willison 2009). Pour ces auteurs, si les études comportementales font aujourd'hui l'objet d'un intérêt accru des chercheurs, des défis significatifs restent encore à surmonter pour faire avancer ce courant de recherche » (Crossler et al. 2013 p. 91). Les pistes de recherche qu'ils indiquent s'inscrivent dans le prolongement de l'amélioration des connaissances des comportements des utilisateurs finaux. Cependant, il est **peu fait cas de l'aspect managérial de la SSI** comme l'évoquent plusieurs autres auteurs (Choobineh et Dhillon 2007 ; Dlamini et al. 2009 ; Goodhue et Straub 1991 ; Kotulic et Clark 2004 ; McFadzean et al. 2007 ; Posthumus et Solms 2004 ; Straub et Welke 1998 ; Solms et Solms 2006a).

Notre thèse a pour ambition de mieux cerner et d'expliquer les éléments considérés lors de la décision d'adopter symboliquement la SSI par les top-managers. Notre problématique et nos questions de recherche s'inscrivent dans le prolongement de plusieurs études académiques sur la relation entre perception des risques et SSI. En ce sens, nous relions nos travaux aux études dans lesquelles sont abordés les concepts que nous mobilisons et plus particulièrement celles qui appellent à les prolonger, sur le champ de la SSI pour 1) **l'implication des dirigeants**, 2) la **perception des risques**, 3) **l'approche socio-organisationnelle** et 4) les **influences externes et internes**.

2.5.1. Implication pour la SSI des dirigeants

S'il a pu être observé que les top-managers, au titre du bon fonctionnement global de l'organisation, acceptent la responsabilité de la SSI, leur manque d'engagement est plus commun, devenant « un des plus grands inconvénients pour obtenir une SSI effective dans la plupart des organisations » (Solms 1996). Selon Barlette et Fomin (2010), les raisons

pouvant expliquer le manque d'implication des top-managers doivent être étudiées spécifiquement. Notamment ils précisent que certains top-managers « **sous-estiment les risques auxquels leur entreprise doit faire face** » et qu'ils accordent davantage d'importance aux risques externes tels les hackers ou les virus qu'aux risques internes tels l'abus d'initié ou l'erreur humaine (Barlette et Fomin 2010 p. 128). Ce commentaire peut être mis en perspective du postulat de Taylor (2006 p. 1582) indiquant les difficultés d'appréciation des risques par les top-managers, basée sur des heuristiques et conduisant à une perception erronée « des risques réels de sécurité de l'information » laissant alors l'organisation exposée à « des menaces graves ». Rappelons que selon Kotulic et Clark (2004) la gestion des risques a justement pour but de « maximiser le gain possible en minimisant la perte possible » par un processus de gestion des risques « qui contribue à l'efficacité globale de l'organisation ». Ils indiquent que, « historiquement, ce processus est considéré par les top-managers uniquement lorsqu'un incident de sécurité est survenu » (Kotulic et Clark 2004 p. 598). Notons que cet avis est partagé par Johnston et Warkentin (2010 p. 551) qui définissent la menace, composant essentiel du risque, comme « un stimulus externe qui existe indépendamment qu'il soit perçu ou non par un individu ». Globalement, les travaux précédents appellent à étudier :

pourquoi les top-managers sous-estiment le risque et sur quels éléments ils fondent leur perception et leur évaluation des risques, ce qui pourrait éclairer la position réactive vis-à-vis de la SSI.

En outre, dans l'alignement avec les travaux de Straub (1990) et Kankanhalli et al. (2003), Barlette et Fomin (2010) évoquent le manque de **connaissance sur les réponses possibles aux risques**. Ce manque peut contribuer à une position réservée pour la SSI dans la mesure où les top-managers ne seraient pas en capacité d'évaluer les avantages à répondre aux risques, soit à choisir et mettre en œuvre justement les mesures de sécurité.

Kankanhalli et al. (2003), à l'appui des travaux d'Eloff (1988), affirment qu'une clé majeure pour la SSI relève de l'engagement des top-managers. Selon ces auteurs, l'engagement des top-managers peut se manifester par une participation active pour la formulation des orientations stratégiques et leurs déclinaisons opérationnelles à la SSI, par exemple lors de l'élaboration de la politique de sécurité. En outre, leur soutien permet un engagement plus appuyé des ressources financières et techniques pour la SSI, conduisant alors à un dispositif de sécurité potentiellement moins exposé aux incidents. S'il semble acquis la nécessité pour

les top-managers d'investir la SSI, Kankanhalli et al. (2003) précisent qu'ils doivent préalablement être **conscients de « l'importance de la sécurité informatique** ». Ils appellent alors à étudier les éventuels liens entre capacité d'avantage stratégique portée par le SI et SSI, notamment en regard des enjeux pour leur organisation. Spécifiquement, concluant sur une gestion des risques plus efficiente lorsque les utilisateurs sont impliqués, Spears et Barki (2010) s'interrogent sur les **influences du contexte d'affaire** dans l'engagement des acteurs pour la SSI. La synthèse des appels de ces travaux pourrait alors conduire à observer l'investissement pour la SSI en regard du niveau stratégique du SI et du secteur d'activité de l'organisation du décideur.

Zafar et Clark (2009) notent la divergence entre la prédominance technique et l'approche holistique de la SSI, qui, cette dernière, retiendrait peu l'intérêt des recherches de la discipline. En effet, selon eux, les organisations ne sont pas encouragées à adopter la SSI. Ce commentaire suggère de s'intéresser aux influences qui pourraient conduire à la mise en œuvre d'une SSI plus globalement, répondant aux enjeux stratégiques de l'organisation. En ce sens Spears et Barki (2010 p. 520) proposent, pour la compréhension de la participation à la gestion des risques SI, de centrer davantage les recherches au niveau individuel pour observer les aspects « **psychologiques et affectifs comme la participation, l'attitude, l'intention et l'acceptation** ».

Knapp et al. (2009), selon une approche socio-organisationnelle développée par Dhillon et Backhouse (2001), précisent l'intérêt du management de la SSI et soulignent la nécessité d'identifier, dans les recherches futures, les facteurs clés de succès des pratiques de sécurité tels l'engagement des managers exécutifs et leurs conséquences sur la politique et la culture organisationnelle de la SSI. Hu et al. (2007 p. 170) établissent justement la relation entre « climat sécurité » et comportement des utilisateurs. En ce sens, ils suggèrent de s'interroger sur les facteurs les plus prégnants conduisant à améliorer globalement la SSI dans l'organisation.

Choobineh et al. (2007) concluent leurs travaux sur l'état des lieux de la recherche SSI en précisant que les décisions des top-managers doivent être explorées pour éclairer le comportement des managers intermédiaires et leur perception des décisions des top-managers.

Enfin, pour McFadzean et al. (2007 p. 655), la majorité des études sont centrées sur des « dispositifs de sécurité structurés pour lesquels les objectifs et rôles sont (*préalablement à l'étude*) définis ». Ils appellent alors à prendre en compte, dans les recherches à venir, les

éléments en amont de ces structures pour identifier précisément les rôles des acteurs pour l'alignement de la stratégie et la SSI. Dans leurs travaux, ils établissent un lien entre les comportements des top-managers et les « impacts sur leurs propres rôles et actions incluant le développement de la stratégie SSI de l'organisation (McFadzean et al. 2007 p. 647). En d'autres termes, il s'agit d'étudier les **facteurs d'influence** qui conditionnent l'articulation du **couple « décision » et « SSI** ».

2.5.2. Manque d'étude sur la perception des risques

La question au cœur de notre étude peut se reformuler en regard de différentes conclusions, convergentes, issues de la littérature sur la décision de protéger le SI : est-il nécessaire, pour l'organisation, de subir un incident majeur avant de prendre les dispositions adaptées pour assurer la protection de son SI ? Particulièrement, Albrechtsen et Hovden (2009) soulignent un manque d'étude sur la **perception et sur le jugement du risque SI**, sur la base de leur étude explorant la différence de perception des risques entre managers et utilisateurs. A l'appui de références académiques de la perception des risques dans la discipline psychologique, telles que Slovic (2000) ou Sjöberg (2002), ils indiquent que le risque peut être perçu différemment selon les caractéristiques idiosyncratiques et les influences externes comme, par exemple, l'avis des experts du domaine (Albrechtsen et Hovden 2009). Notons qu'Albrechtsen (2007), dans ses travaux précédents, avait déjà constaté la relation étroite entre perception des risques et vision de la SSI par les acteurs. Également, Albrechtsen et Hovden (2009 p. 486) appellent à étudier la décision individuelle de la SSI en regard des contre-mesures possibles et choisies.

Choobineh et al. (2007 p. 967) précisent que les recherches à venir puissent renforcer les cadres théoriques de la SSI en **mobilisant d'autres disciplines**, comme la stratégie d'entreprise et **la psychologie**, afin d'expliquer, notamment, pourquoi la sécurité n'est pas développée en parallèle des SI, « aboutissant à un système globalement moins sécurisé ». Dans cette perspective, Warkentin et Willison (2009 p. 102) soulignent qu'au-delà des recherches portant sur le comportement des acteurs dans le champ de la SSI, appuyés par des cadres théoriques éprouvés tels que TAM, ils appellent à explorer la discipline selon de **« nouvelles fondations théoriques »** pour « apprendre d'autres **sciences cognitives et comportementales** ».

Bandyopadhyay et al. (1999 p. 440) ont eu pour projet d'élaborer un cadre de gestion des risques SI après avoir démontré **la faible utilisation de méthode d'analyse de risque**

structurée d'une part, mais aussi en soulignant une gestion des risques bâtie sur la **« perception de leurs directeurs ».** Ainsi, ils appellent à éclairer le cadre de gestion des risques qu'ils ont développé et proposent d'étudier la perception des conséquences sur l'organisation elle-même et son environnement.

Crossler et al. (2013 p. 97), parmi les cinq nouvelles voies pour la recherche en SSI visant à améliorer la conformité à la SSI, indiquent notamment qu'il faudrait « distinguer la crainte en tant qu'émotion de la crainte en tant que connaissance ». Cela appelle alors à étudier quelles influences constituent la crainte avant de savoir s'il s'agit d'émotion, de connaissance, ou d'une articulation des deux. L'étude de Vance et al. (2014 p. 683) traite justement de la sensibilité aux messages d'alertes. Selon ces auteurs et en accord avec les découvertes de Johnston et Warkentin (2010), l'accoutumance des utilisateurs aux messages d'alerte diminue leur perception du risque **lorsque le message d'alerte ne se traduit pas par des conséquences négatives**. Vance et al. (2014) parlent d'ici d'un phénomène nommé « crier au loup ».

2.5.3. Approche socio-organisationnelle

Alors qu'« une grande partie des recherches se centrent sur les problèmes techniques » (Crossler et al. 2013), plusieurs auteurs évoquent l'humain comme faiblesse majeure dans le dispositif de protection de l'information (Albrechtsen et Hovden 2009 ; Dhillon et Backhouse 2001 ; Siponen and Oinas-Kukkonen 2007 ; Vroom et Solms 2004 ; Warkentin et Willison 2009). Ainsi l'approche socio-organisationnelle a été développée initialement par Dhillon et Backhouse (2001) sur la base de leur analyse, des préoccupations socio-philosophiques pour les SI et leur sécurité d'une part et d'une critique nourrie pour les seules considérations techniques d'autre part. Ils se sont appuyés sur des problèmes d'intégration de la sécurité dans deux organisations afin d'étayer la nécessité de considérer les **aspects sociaux et politiques** pour aborder la SSI qui « semblent avoir un impact significatif sur la façon dont les SI sont conçus et mis en œuvre ». Dhillon et Backhouse (2001 p. 137) dressent une synthèse prospective, appelant à être vérifiée, spécifique à l'analyse de risque. Selon eux, le cadre conceptuel avec lequel serait abordé l'ensemble des questions de sécurité est très limité car construit sur **deux prémices non-fondées**. D'abord, par manque d'une **vision holistique de la SSI**, une distinction clivante entre organisation, environnement et SI, implique une faible considération des exigences liées aux activités majeures.

Ensuite, les apports des SI, et ainsi de la SSI, sont observés comme résultat d'un processus, alors que les **bénéfices de la SSI sont difficilement quantifiables**, ce qui peut conduire à un désintérêt pour cette activité. Nous soutenons, que ces hypothèses peuvent être éclairées selon une approche de gestion des risques, par des acteurs disposant d'une vision « métier » et globale de leur organisation, soit les top-managers. Choobineh et Dhillon (2007 p. 961) prolongent l'appel de Dhillon et Backhouse (2001) et précisent **qu'après des décennies de recherche théorique et pratique, le management de la SSI est encore souvent considéré après coup dans les organisations**. Ils confirment la nécessité de dépasser la dualité entre activités majeures et SI dans l'approche de gestion des risques. Ils appellent alors à décrire les mécanismes sur lesquels est fondée la gestion du risque, considérant isolément la conception et le développement des SI en parallèle de la SSI plutôt que de manière intégrée.

McFadzean et al. (2007) ont démontré la relation entre la valeur stratégique du SI dans les organisations et la vision des top-managers sur la SSI, rejoignant les commentaires de Kankanhalli et al. (2003). Également à l'appui des travaux de Dhillon et Backhouse, (2001) McFadzean et al. (2007) considèrent les questions sociales comme un composant central dans la sécurité de l'information et l'analyse de risque. Ils suggèrent d'entreprendre des recherches plus approfondies sur, notamment, la **perception de risque et les rôles**, formels et informels, dans la SSI et les processus d'analyse de risque, selon une « perspective d'alignement de la SSI sur la stratégie SI de l'organisation » (McFadzean et al. 2007 p. 655).

Pour Soomro et al. (2016) la littérature met l'accent sur le facteur humain dans la SSI pour son rôle majeur dans les infractions commises sur le SI et, à l'inverse, pour le respect des règles quant au comportement attendu par l'organisation. En admettant qu'il s'agit de deux points critiques pour le management de la SSI, ces auteurs appellent à étendre le champ de la recherche à toutes les activités qui ont un impact significatif sur la SSI et particulièrement celles dont la direction est directement responsable. Suggérant d'adopter une approche plus holistique au management de la sécurité de l'information (Soomro et al. 2016) il s'agit, en regard de notre projet de recherche, d'explorer justement les influences de la décision d'adopter symboliquement la SSI. Dans cette perspective, Hu et al. (2007 p. 155) constatent que les études en sécurité des systèmes d'information ne sont pas adossées à « des cadres théoriques forts » et préconisent « un cadre socio-organisationnel plus cohérent » pour expliquer notamment comment **sont développées les croyances des top-managers** et également comment elles « **peuvent être influencées et changées** ». Les travaux de Hu et al. (2012) prolongent cette perspective en indiquant qu'un des principaux défis pour le

mangement de la SSI est de comprendre de quelle façon il est conditionné par l'articulation de l'organisation, des individus et des techniques. En effet, la culture organisationnelle et la participation des tops-managers influencent la culture sécurité de l'entreprise, qui a elle-même un effet significatif sur l'ensemble des acteurs (Hu et al. 2012).

2.5.4. Application de la théorie néo-institutionnelle

McFadzean et al. (2007), après avoir précisé que la perception des top-managers implique l'articulation d'informations provenant de l'organisation, des croyances et des valeurs, soulignent l'impact de ces influences sur leurs rôles et leurs actions. Leurs rôles sont alors influencés, de fait, lorsqu'il s'agit du « développement de la stratégie de sécurité de l'information de l'organisation » (McFadzean et al. 2007 p. 647). Ainsi, Hu et al. (2007), sur la base des travaux de Dhillon and Backhouse (2001), présentent la théorie néo-institutionnelle comme « parfaitement adaptée pour expliquer comment les facteurs institutionnels influencent le comportement des acteurs de l'organisation ». Après avoir mis en perspective les influences coercitives et normatives pour deux compagnies soumises à SOX, ils appellent à comparer leurs résultats avec des compagnies dont les activités sont différentes (Hu et al. 2007). Dans ce prolongement, Kwon et Johnson (2014) ont étudié les effets de la réglementation sur les apports pour la SSI et soulignent qu'un investissement proactif pour la SSI est associé avec des incidents moindres. Cependant, ils remarquent une différence entre influences externes et coercitives dans le cas étudié et donc imposées, et les influences internes qui peuvent conduire à des mesures préventives volontaires, développées par l'organisation, qui en seraient alors plus efficaces. Ils précisent que l'efficacité doit être considérée dans la prise de décision car elle « est particulièrement importante pour des organisations opérant avec des ressources contraintes et des menaces en évolution » (Kwon et Johnson 2014 p. 467). Ils précisent alors la nécessité d'observer la combinaison des pressions externes et internes pour expliquer leurs effets sur la mise en œuvre de la SSI.

2.6. Questions de recherche

À notre connaissance, la faible perception des risques SI des top-managers n'a été que peu étudiée, peut-être à cause de la sensibilité et de la « confidentialité » du sujet (Loch et al.

1992 p. 177[22] ; Kotulik et Clark 2004). Au regard de ces constats et de notre problématique, nous nous interrogeons justement sur la décision des top-managers d'investir la SSI afin d'éviter les conséquences pour leur organisation et des écueils pour eux. Nous pouvons alors formuler notre première question de recherche :

Quels sont les éléments considérés dans la décision d'adopter symboliquement la SSI ?

La littérature traitant du thème « conformité » montre les forces majeures s'exerçant sur l'organisation et ses décideurs quant à la nécessité de la SSI. Outre l'isomorphisme coercitif, imposant à l'organisation la mise en œuvre d'une SSI « normée », nous nous intéressons davantage aux influences normatives et mimétiques. En effet, plusieurs auteurs ont mis en évidence cette influence enjoignant les décideurs à s'intéresser à la SSI. Par exemple la crainte de perte d'image suite à une potentielle divulgation de données confidentielles (Kwon et Johnson 2014), aurait des conséquences directes sur l'organisation des décideurs ; constatant cette possible déconvenue pour eux et leur propre organisation, refusant de subir de telles conséquences, les décideurs considèreraient alors davantage les réponses possibles pour y faire face.

Les influences sur la SSI peuvent être observées selon deux aspects, tous deux centraux à la gestion des risques (Liang et Xue 2009) : **l'évaluation de la menace** et **l'évaluation de la réponse possible** à cette menace. L'évaluation de la menace est similaire à l'évaluation du risque, traité dans le paragraphe précédent et objet principal de notre première question de recherche. L'évaluation de la réponse s'inscrit dans la recherche de solutions activables auprès des organisations spécialisées, des associations, des groupes d'industrie et de « l'opinion publique » (Di Maggio et Powell 1983). Avec des pressions normatives, des choix organisationnels sont influencés par des valeurs et des normes. Les organisations se conforment par l'obligation morale et éthique en fonction de ce qu'elles croient qu'on attend d'elles (Scott 1995). En ce sens Williams et al. (2009) ont démontré les influences isomorphiques qui peuvent pousser les organisations à mettre en œuvre un dispositif de sécurité. Si la pression coercitive est le moteur principal dans l'organisation qu'ils ont étudié, les pressions mimétiques et normatives ont largement contribué à la mise en place de

[22] Loch et al. (1992) précisent la sensibilité du sujet de la sécurité qu'ils évoquent comme raison d'un faible retour à leurs questions pour lesquelles ils ont obtenu 20% de réponses.

procédures et mesures renforçant la sécurité de la chaine d'approvisionnement (Williams et al. 2009).

D'autres auteurs ont évoqué les influences liées aux décisions managériales de la SSI. Par exemple, Karyda et al. (2005) soulignent la relation étroite entre caractéristiques idiosyncratiques (expériences, connaissance, objectifs et priorités, rejoignant ainsi partiellement les résultats de Goodhue et Straub, 1991) et compréhension du besoin SSI. Tsohou et al. (2006) ont établi une relation entre théorie culturelle du risque et méthode pratiquée pour analyser et traiter les risques SI. Enfin, Hu et al. (2007) ont démontré les apports mutuels entre top-managers et acteurs pour accroitre la maturité de la sécurité d'une organisation, nous conduisant à observer les influences internes pour l'adoption symbolique de la SSI.

Considérant que les décisions quant à la SSI se font selon des influences propres (perception des risques) et aussi selon des influences externes et internes, notre deuxième question de recherche peut alors se formuler ainsi :

Comment ces éléments influencent la décision d'adopter symboliquement la SSI ?

2.7. Conclusion du chapitre

L'analyse de la littérature a mis en perspective l'importance de la sécurité des SI et ses implications pour les organisations. Une fois établi le triangle « stratégie », « système d'information » et « sécurité », nous comprenons aisément que la SSI, centrée sur les activités majeures de l'organisation, ait un rôle critique dans le succès des sociétés (Soomro et al. 2016).

La dépendance des organisations à leur SI appelle une attention particulière pour la sécurité. Les conséquences des incidents de sécurité dépassent le plan technique pour impacter le fonctionnement même des organisations, leur stratégie et leurs dirigeants. Goodhue et Straub (1991) ont démontré, il y a plus de deux décennies, la faible considération des top-managers avant que ne survienne un incident de sécurité majeur. Nous avons présenté les travaux de plusieurs auteurs qui, depuis et jusqu'à ce jour, établissent des conclusions convergentes sur **la faible implication des top-managers pour la SSI** (Choobineh et Dhillon 2007 ; Doherty et Fulford 2006 ; Goodhue et Straub 1991 ; Hagen et al. 2008 ; Kotulik et Clark 2004 ; Kwon et Johnson 2014 ; McFadzean et al. 2007). En complément, il fait

consensus dans la littérature que la SSI doit aujourd'hui relever d'une responsabilité de direction générale (Hu et al. 2007 ; Solms et Solms 2006b) ce qui implique de la considérer selon une approche « top-down ». D'une part, il apparait que les directeurs ont la nécessité de disposer de SI pérennes et fiables pour assurer les activités dont ils ont la responsabilité. Le corolaire de ce constat est qu'en l'absence de protection ils auraient à subir directement les impacts d'un incident SI (Moulton et Coles 2003). D'autre part, l'engagement du plus haut niveau de l'organisation assure d'articuler vision stratégique et SSI (Posthumus et Solms 2004), de disposer d'un dispositif de protection centré prioritairement sur les activités majeures (McFadzean et al. 2007), de pouvoir adapter le changement de culture sécurité (Hu et al. 2007 ; Knapp et al. 2006) et enfin, d'engager les moyens et ressources nécessaires à la conception et l'élaboration d'un dispositif de SSI (Barlette et Fomin 2010).

Le manque d'implication des directeurs et top-managers pour la SSI, identifié dans les conclusions des travaux empiriques et mis en perspective des rôles définis pour les directeurs et top-managers, restent une question pertinente et non résolue. Pour Kankanhalli et al. (2003 p. 140) si la question de la SSI est cruciale, l'attention portée à ce sujet est « anormalement basse comparée à d'autres questions SI ». Plusieurs hypothèses sont évoquées pour expliquer le manque de considération de la SSI telles que par exemple la prédominance technique ou **la faible perception des risques SI.**

La SSI a longtemps été considérée comme une problématique technique, sans doute parce que le SI était lui-même observé comme un assemblage de briques « IT » sans considération « organisationnelle ». Ceci peut effectivement expliquer l'orientation des top-managers à déléguer cette responsabilité aux experts techniques (Choobineh et Dhillon 2007 ; Hagen et al. 2008), en écartant alors l'aspect stratégique de la problématique. La littérature fait aujourd'hui consensus sur la nécessité d'articuler SSI et stratégie (Posthumus et Solms 2004 ; Silic et Back 2014), limitant alors l'intérêt pour cette hypothèse.

Nous avons fait émerger des travaux académiques les enjeux de la SSI pour l'organisation et également pour les top-managers. Ces enjeux, quel que soit le thème de la littérature sur la sécurité, tel que par exemple la gouvernance ou la conformité, peuvent s'articuler autour de la gestion des risques pour les organisations et les top-managers. En effet, que nous considérions les risques SI en regard de l'impossibilité de réaliser les activités ou la non-conformité aux lois et règlements, les conséquences dépassent le plan technique du SI pour atteindre l'organisation dans son ensemble et ses top-managers. Cependant, les thèmes « gouvernance » et « analyse de risque » donnent une perspective particulière sur la **faible perception des risques SI des top-managers**. Selon les tops-managers, il n'est pas toujours

nécessaire d'élaborer un dispositif de sécurité car **les SI sont faiblement exposés aux risques** (Kankanhalli et al. 2003). D'autre part, les tops-managers ne sont pas assurés de l'efficacité des mesures constitutives de ce dispositif (op. cit.).

Ces commentaires peuvent être rapprochés de la difficulté d'appréhender les risques lorsqu'il n'est encore « **rien n'est arrivé »** (Kwon et Johnson 2014 p. 452). En effet, si la « réussite de la SSI » peut se mesurer justement parce qu'il n'y a eu aucune conséquence ou incident (Hu et al. 2007), la réciproque peut être considérée : **il n'est rien arrivé, alors investir la SSI n'est pas nécessaire**. Rappelons ici que, selon Gerber et Solms (2005), le risque lui-même est un concept complexe en ce sens qu'il comprend une combinaison d'éléments. En complément Tsohou et al. (2006) précisent que le risque est un concept abstrait puisqu'il n'a pas de matérialité, rejoignant l'idée que le concept de risque est peu accessible lorsqu'aucun incident n'est survenu (Kwon et al. 2012). En effet, Hu et al. (2007 p. 166) précisent que la réussite de la SSI se traduit par l'absence de conséquence, rendant alors délicates les évaluations économiques de son avantage ou de l'absence de pertes puisqu'il s'agirait alors d'observer des résultats intangibles tels que, par exemple, les avantages de la conformité réglementaire, la « crédibilité publique » ou des gains sur l'image de marque.

Pour étayer davantage notre propos, nous pouvons citer l'étude prédictive des comportements des acteurs finaux pour la SSI. Face à un risque quant à l'usage des SI et les pratiques de SSI, il a été observé que les acteurs ne considèrent cette situation comme **un risque avéré que lorsqu'il survient** (Vance et al. 2014). Ce constat est en ligne avec celui d'autres auteurs en SSI (tels que par exemple Kwon et Johnson 2014) et également dans la discipline psychologique de gestion du risque (tels que par exemple Kouabénan 2007, Lichtenstein et al. 1978 ou Sjöberg et al. 2004).

Selon Yates et Stone (1992), s'engager dans une situation « risquée » est une **décision** pour laquelle l'activité conduira à **l'atteinte d'un objectif satisfaisant**. L'atteinte de cet objectif est une décision réussie, à l'inverse, ce serait un échec. En ce sens, Bandyopadhyay et al. (1999), à l'appui des travaux de March et Shapira (1987), concluent que les organisations traitent le risque selon l'importance perçue de ces risques par leurs directeurs. Ainsi, les perceptions des risques observées sont « très différentes des concepts théoriques de risque qui impliquent l'évaluation des probabilités de résultats possibles et le choix parmi des actions alternatives » (Bandyopadhyay et al. 1999 p. 440). Or, dans une perspective où les SI sont stratégiques (Kankanhalli et al. 2003 ; Kayworth et Whitten 2010) tout en étant exposés à des menaces pouvant obérer le succès des sociétés (Soomro et al. 2016), la décision de

protéger les SI devient centrale pour ceux qui en ont la responsabilité. Nous soutenons alors que la volonté de **s'engager dans la protection du SI relève d'une décision**, qui pourrait conduire à un niveau de sécurité permettant de réduire la survenance d'un risque ou d'en limiter les conséquences (Choobineh et Dhillon 2007). Cette décision résulte d'une conjugaison d'influences qui ne sont, à notre connaissance pour la SSI, que peu étudiées dans la littérature.

Enfin, la littérature SSI pose comme étape fondamentale l'analyse de risque, première brique du dispositif de sécurité des systèmes d'information. Elle permet d'objectiver les risques menaces, probabilité et conséquences, conduisant ensuite à l'implémentation, l'organisation et le contrôle de mesures de sécurité. Si l'étape d'analyse de risque est appelée par le management de la SSI, alors nous pouvons nous interroger sur les risques analysés en amont de son adoption, a minima les risques considérés pour justement l'initier, ce qui implique ensuite de réaliser une analyse « formelle » des risques permettant, *in fine,* de structurer le dispositif de SSI de l'organisation.

La figure 7 présente un synoptique des concepts mobilisés pour le projet tel que nous l'avons élaboré à partir de la littérature et centré sur l'adoption symbolique de la SSI par les top-managers.

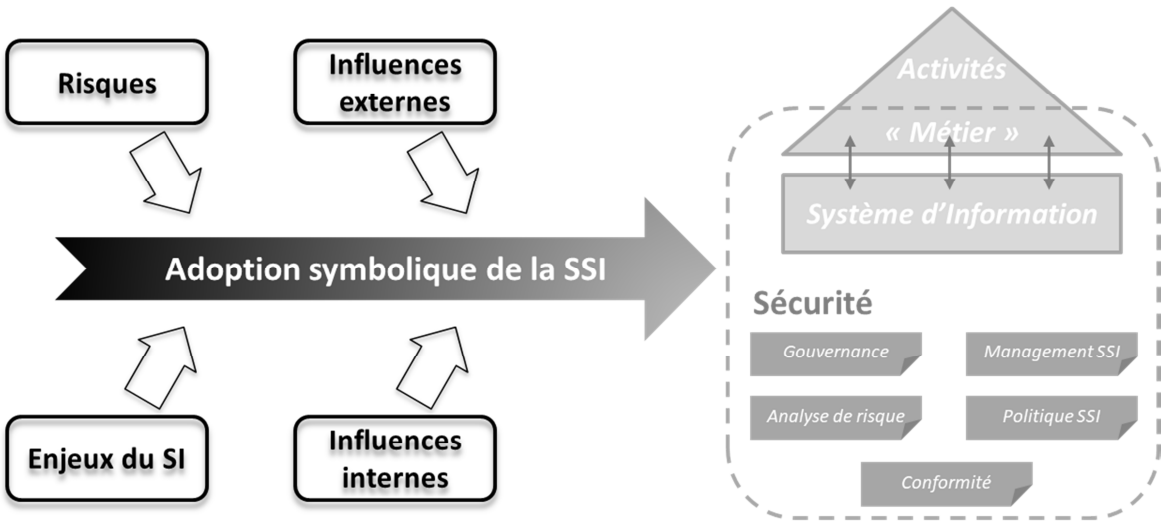


Figure 7 : Synoptique intermédiaire de notre recherche

Chapitre 3. Cadre théorique pour l'adoption symbolique

Notre projet consiste à comprendre les **influences considérées** pour décider d'initialiser la SSI. Nous mobilisons un cadre théorique d'adoption symbolique (AS) qui permet d'étudier ces influences lors de l'élaboration de la décision. Spécifiquement, ce cadre se définit comme « l'acceptation du composant d'idée d'une innovation, ou la décision qu'une innovation est appropriée » pour le décideur (Klonglan et Coward 1970 p. 82) permettant alors d'étudier l'ensemble des éléments mobilisés. L'AS est particulièrement adapté à notre problématique car nous centrons nos observations sur la décision d'adopter non pas l'adoption matérielle, mais l'adoption de l'idée, permettant alors d'écarter les considérations économiques et de mise en œuvre pratique. Initialement établi pour étudier l'adoption d'innovation, nous adaptons ce cadre à la SSI, en faisant interagir trois champs théoriques, que sont la perception des risques, la sécurité de l'information et le néo-institutionnalisme.

Selon Hameed et al. (2012 p. 360), les recherches sur l'innovation portent sur « la compréhension et l'examen des déterminants organisationnels d'adoption d'innovation et les effets d'adoption d'innovation sur la performance organisationnelle ». Ces recherches distinguent deux courants d'adoption d'innovation : le comportement des organisations quant à son expérience d'adoption et **les attributs qui influencent l'adoption** (Hameed et al. 2012). Nos travaux visent à rendre intelligible les éléments considérés lors de la décision d'adopter symboliquement la SSI aussi nous nous concentrerons sur les facteurs d'adoption que nous situerons dans le processus d'adoption pour appréhender les éventuelles interactions.

Les recherches sur l'adoption d'innovation peuvent permettre d'étudier le niveau individuel, de groupe ou d'organisation (Hameed et al. 2012). Si ces trois niveaux sont parfois imbriqués, nous nous **intéressons principalement au niveau individuel**, objet de notre étude sur l'adoption symbolique.

3.1. Le modèle d'adoption symbolique

La littérature sur l'adoption des SI mobilise majoritairement des modèles ancrés dans les théories de l'action raisonnée, du comportement planifié, de la diffusion de l'innovation, et de la théorie cognitive sociale. Le modèle de l'acceptation de la technologie (TAM) et ses révisions (TAM2 et TAM3), ainsi que la théorie unifiée de l'acceptation et de l'utilisation de la technologie (UTAUT) contribuent à expliquer et prédire l'adoption des SI par les acteurs.

Dans ces modèles, l'utilisation technologique est prévue en fonction des intentions d'exécuter un tel comportement. L'intention d'usage, quant à elle, est le résultat de l'attitude envers le comportement, soit l'utilité et la facilité d'emploi perçue dans le cas de TAM et des attitudes et la norme subjective dans le cas de TRA. Ainsi, Nah et al. 2004 (p. 35) précisent la similarité entre les modèles TAM et diffusion de l'innovation (Rogers 1983, 2003) car, selon ces auteurs, « l'utilité perçue et la facilité d'utilisation perçue sont semblables à l'avantage relatif perçu » et à « la complexité perçue ». Ces modèles, déterministes, expliquent l'acceptation[23] selon les caractéristiques de la technologie et leur perception, quels que soient les utilisateurs et les contextes. En effet, il s'agit pour les acteurs de « construire » leur intention d'utiliser une technologie en regard de caractéristiques identifiées qu'ils connaissent et formalisent pour prédire l'adoption. Ainsi, d'une part, ces modèles ne peuvent permettre l'exploration de l'adoption d'une technologie comme « bonne idée » sans considération de leur déclinaison pratique (usage). D'autre part, sur un postulat volontariste d'usage, ce modèles ne peuvent considérer les influences coercitives qui à l'inverse, émergeraient dans un contexte où l'usage d'une technologie devient obligatoire. En outre, dans la littérature SSI, certains auteurs tels que par exemple Warkentin et Willison (2009 p. 102) soulignent qu'au-delà des recherches portant sur le comportement des acteurs dans le champ de la SSI, appuyés par des cadres théoriques éprouvés tels que TAM, et appellent à explorer la discipline avec de « nouvelles fondations théoriques » en intégrant d'autres sciences cognitives et comportementales.

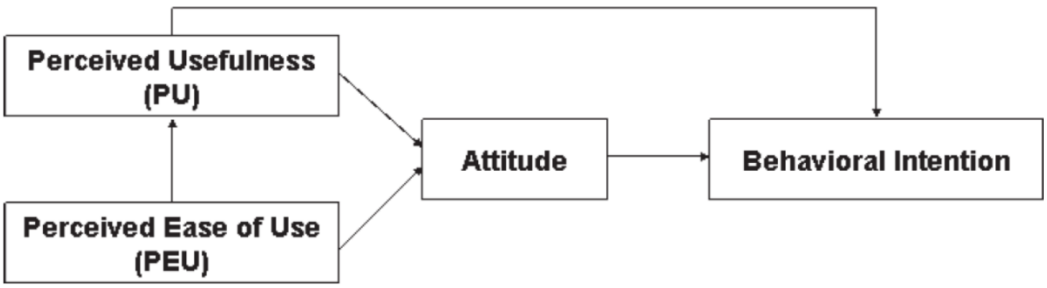


Figure 8 : Formulation initiale du modèle TAM

(Nah et al. 2004 p. 35)

[23] Selon Venkatesh et Davis (2000) TAM permet d'expliquer environ 40 % du désaccord dans des intentions d'utilisation et le comportement.

Motivés par la découverte des influences symboliques pour l'adoption de la SSI, nous préférons alors mobiliser un cadre théorique qui permet d'**observer la décision de la SSI sur un plan purement réflexif**, écartant les considérations matérielles, soit **l'adoption symbolique de Klonglan et Coward (1970).**

3.1.1. L'adoption symbolique : étude des décisions d'adoption d'innovation

Les travaux de Klonglan et Coward (1970) s'inscrivent dans la théorie de la diffusion d'innovation (Rogers 1962). Selon Karahanna et al. (1999 p. 185), sur la base des travaux de Rogers (1983), le processus de décision d'innovation conduisant à l'institutionnalisation de l'usage peut être « conceptualisé comme **un ordre temporel d'étapes** par lesquelles un individu passe de la connaissance initiale d'une innovation, à la formation d'une attitude favorable ou défavorable envers elle, à une décision d'adopter ou de rejeter la mise en œuvre l'innovation ».

Klonglan et Coward (1970) appuient leur théorie sur la distinction entre l'adoption d'une idée et d'un produit ou d'une pratique. Ils précisent qu'une « innovation peut avoir un composant d'idée sans nécessairement avoir un composant matériel », alors que la réciproque n'est pas vraie, le composant matériel ne peut exister sans composant d'idée (Klonglan et Coward 1970 p. 78). Ils soutiennent que tout nouvel artefact ou idée implique autant le **composant d'idée** que le **composant d'objet**, « correspondant respectivement à la **symbolique** et aux formes d'**actions d'adoption** » (Karahanna et Agarwal 2006 p 5). Dans cette perspective, l'adoption d'une innovation technologique nécessite l'interaction de l'adoption mentale, soit le composant conceptuel de l'innovation, et de l'adoption matérielle, soit le composant « artefact ». Selon ces auteurs, les études réalisées jusqu'alors tenaient pour implicite l'étape d'adoption mentale, nommée **adoption symbolique** (AS). La littérature antérieure avait utilisé le terme d'« adoption symbolique » pour se référer à l'acceptation d'une idée immatérielle, plutôt qu'une phase dans le processus d'adoption (Klonglan et Coward 1970 p. 77). Ce constat conduit Klonglan et Coward (1970) à proposer l'AS dans un modèle de processus d'adoption, composé de deux phases.

La première phase, située au cœur de nos travaux, traite de l'adoption du concept alors que la deuxième phase considère l'adoption d'usage. La figure 9 présente un synoptique de leur modèle, permettant de distinguer, dans le processus d'adoption, les éléments relevant de l'acceptation de l'idée (phase A, soit l'adoption symbolique), de ceux de l'adoption d'utilisation, dans laquelle l'objet matériel ou la pratique sont acceptés (phase B, soit

l'essayabilité). En ce sens, les travaux de Klonglan et Coward trouvent une justification empirique dans le champ des SI avec l'étude de Karahanna (1999) qui démontre que l'adoption symbolique précède l'adoption réelle, qu'il s'agit d'une condition nécessaire mais insuffisante pour l'adoption réelle dans des contextes volontaires.

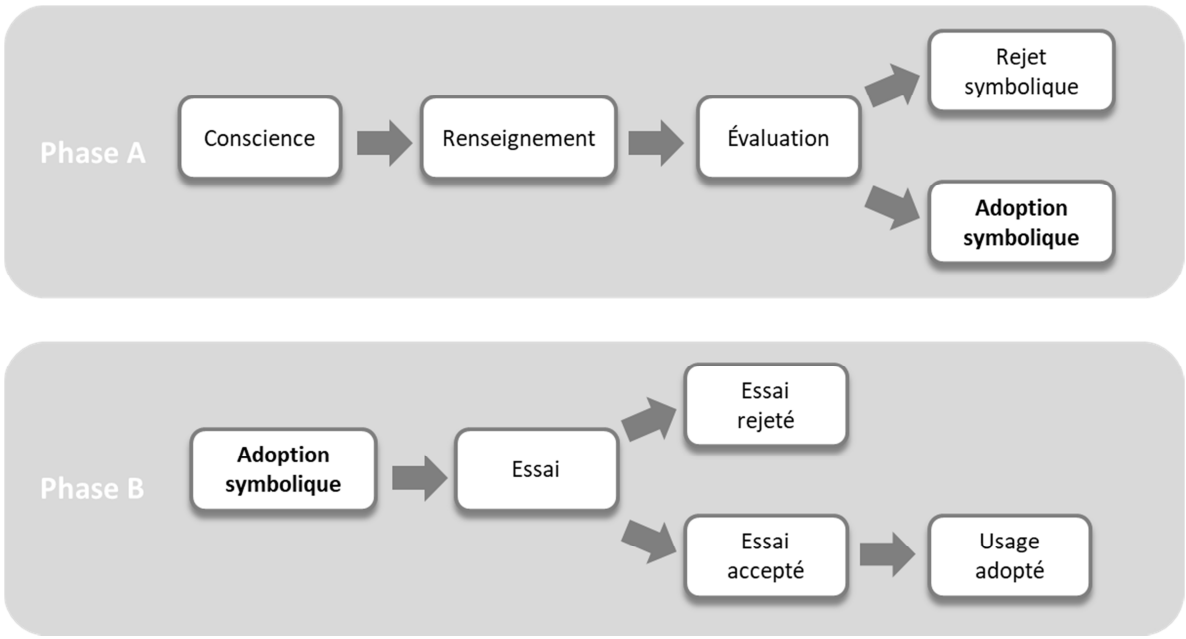


Figure 9 : Place de l'AS dans le processus d'adoption
(Klonglan et Coward 1970 p. 80)

Klonglan et Coward (1970) soulignent que ce modèle à deux phases permet de considérer la **latence observée** empiriquement entre **l'acceptation mentale** d'une idée ou d'une pratique et **la mise en œuvre** matérielle de cette même idée. D'une part, le modèle peut permettre d'expliquer l'adoption ou le rejet en explorant la latence entre adoption symbolique et adoption d'usage, notion que nous précisons davantage dans la présentation du modèle d'adoption de Klonglan et Coward (1970). D'autre part cette latence peut être étudiée en regard des **influences considérées** pour la décision d'adoption d'une nouvelle pratique ou idée. En effet, la latence entre les deux phases peut permettre d'expliquer l'adoption **via des facteurs externes** à l'individu, en plus des facteurs sociologiques ou économiques (Sapp et Korsching 2004). En effet, pour l'adoption, **les variables sociologiques seraient supérieures aux variables économiques** dans l'explication de l'adoption initiale, mais des variables économiques expliqueraient davantage l'institutionnalisation de l'usage (Lesca et al. 2015 ; Karahanna et al. 1999 ; Karahanna et Agarwal 2006 ; Verra et al. 2012). Pour Sapp

et Korsching (2004), l'AS définit un point d'attention majeur dans le processus d'adoption car il valide l'acceptation des principes de l'innovation (renseignements, évaluation et acceptation). Ces mêmes auteurs prolongent ce constat en marquant la différence entre adoption symbolique et adoption. Pour eux, la mise en œuvre qui suit l'adoption entrainent « des considérations de disponibilité, d'essayabilité, des ressources financières et une assistance technique » alors que l'AS représente « les **réponses émotionnelles et affectives** de l'individu aux messages de l'information, la persuasion sociale et des croyances normatives perçues » (Sapp et Korsching 2004 p. 352).

En synthèse, Lesca et al. (2015) soulignent la pertinence de l'AS pour les travaux de pré-adoption. Selon eux, ce cadre théorique permet justement de distinguer le composant d'idée du composant matériel, pour observer l'adoption de la seule idée, sans nécessairement considérer l'usage et les contraintes liées à son institutionnalisation. En ce sens, l'adoption symbolique se présente comme une condition préalable et nécessaire à l'adoption « matérielle ». Lesca et al. (2015 p. 14) précisent dans leurs travaux d'adoption d'un SI, à l'appui des travaux de Klonglan et Coward (1970) et de Sapp et Korsching (2004), que le modèle d'AS « montre que, pour décider d'adopter un SI, il faut au préalable que les individus prennent **conscience** de l'existence de celui-ci, qu'ils **s'informent** et se **renseignent**, qu'ils en **évaluent la pertinence** par rapport à leurs besoins, et finalement qu'ils acceptent mentalement (*symboliquement*) l'idée de l'adopter ».

Afin d'explorer le modèle et exposer la justification de sa mobilisation pour nos travaux, nous développons les concepts sous-jacents et les étapes de la phase A du modèle d'adoption, l'adoption symbolique.

3.1.2. Concepts sous-jacents de l'adoption symbolique

Si le modèle d'AS peut permettre d'éclairer l'adoption de l'idée, il se situe dans un cadre théorique d'adoption de l'innovation à partir duquel il a été construit (Klonglan et Coward 1970). La phase d'adoption débute par la prise de conscience de l'innovation, suivie de son évaluation mentale pouvant conduire à l'acceptation ou au rejet symbolique. Lorsque l'acceptation symbolique est acquise, il s'agit de réaliser un essai d'utilisation matérielle, mentionné parfois comme essai de mise en œuvre. Après une période d'essai, l'innovation

peut être rejetée ou acceptée, conduisant, pour cette dernière option, à l'adoption d'usage, aussi mentionnée comme l'utilisation continue (Klonglan et Coward 1970).

Nous rappelons que nos travaux sont centrés sur l'adoption symbolique (phase A du modèle), ce qui nous conduit à écarter la deuxième phase, l'adoption d'usage. En effet, nous avons développé dans notre problématique (cf. 1.1.4 « Positionnement de notre recherche et problématique » p. 16) les motivations amenant à écarter la phase l'adoption d'usage en regard de notre projet. Nos travaux sont centrés sur l'acceptation mentale de l''idée, ce qui permet alors d'écarter la phase de mise en œuvre avec ses contraintes économiques et ses aspects pratiques. En effet, la prise en compte des considérations économiques pourrait conduire à une acceptation ou à un rejet de la mise en œuvre de la SSI, indépendamment de l'acceptation initiale de l'idée.

Klonglan et Coward (1970) précisent quatre états pour caractériser l'adoption : 1) la connaissance initiale d'une pratique, 2) l'acceptation de la pratique comme bonne idée, 3) l'acceptation de la pratique en essai et 4) l'adoption de la pratique. À notre connaissance, dans la discipline des systèmes d'information, Karahanna (1997 et 1999) et Karahanna et al. (1999) sont les premiers à mobiliser le concept d'AS pour expliquer les différences entre les croyances de pré et de post adoption en SI. Karahanna et al. (1999) appuient leurs travaux sur l'importance du processus d'adoption. Ils constatent le peu d'études distinguant les croyances et des attitudes de pré-adoption et celles d'adoption d'usage, en soulignant que cette distinction est cruciale dans la compréhension du processus d'adoption. Ensuite, Karahanna et Agarwal (2006 p. 8) ont prolongé le concept d'AS en définissant « l'adoption symbolique d'une technologie comme un état maximal de motivation relevant de l'évaluation mentale d'un utilisateur de la technologie et son utilisation comme un concept **digne d'intérêt** ». En introduisant la notion de motivation, Karahanna et Agarwal (2006 p. 8) précisent alors le modèle d'AS par 1) « l'acceptation mentale, capturant la mesure avec laquelle un utilisateur voit l'artefact, en principe, comme une bonne idée, 2) l'engagement d'utilisation, représentant le degré de volonté pour utiliser la technologie, indépendant de son caractère obligatoire ou non, 3) le mérite d'effort, ou l'évaluation positive de l'utilisateur du retour sur des ressources dépensées pour pouvoir utiliser la technologie et 4) l'enthousiasme intensifié, capturant l'ardeur avec laquelle un utilisateur s'approche des comportements associés à l'utilisation de la technologie ». Si l'intitulé des phases est sensiblement différent dans les travaux de Klonglan et Coward (1970), nous observons dans le modèle revu de Karahanna et Agarwal (2006), que la phase d'adoption symbolique relève uniquement de l'état 1 et 2 (acceptation mentale et engagement à utiliser l'innovation). Ce

constat est concordant avec les remarques de Rawstorne et al. (1998), précisant que l'AS diffère de l'intention d'adoption d'usage. Par exemple, comme indiqué au début de cette section, Karahanna et Agarwal (2006) mesurent l'intention d'adoption d'usage avec l'AS, en intégrant dans leur modèle l'intention d'usage. Précisément, la mesure d'intention d'adopter des utilisateurs s'effectue en évaluant leur intention d'utiliser le SI. Karahanna (1997) a mesuré l'AS en demandant aux utilisateurs d'évaluer des « variables affectives », telles que le « mérite d'effort »[24] et « l'enthousiasme intensifiés »[25] (Karahanna et Agarwal 2006 p. 8) par rapport à leur **utilisation prévue** du SI. Pour ces auteurs, l'adoption symbolique **reflète un état « d'enthousiasme intensifié »** et **« l'excitation pour la technologie »** car ce ne sont pas « un aspect de la construction de participation d'utilisateur », les replaçant alors dans les influences de pré-adoption (Karahanna et Agarwal 2006 p. 9). L'extension du modèle d'AS réalisée par Karahanna et Agarwal (2006), se comprend en regard de leurs objectifs de recherche. Ils mobilisent le cadre d'adoption symbolique pour expliquer les comportements d'usage de la technologie et l'exploration à l'appui de TRA[26] et TAM[27]. Leur volonté d'adapter un modèle théorique compatible avec l'attitude de croyance les écarte du modèle d'AS. Ainsi, ils incluent deux croyances comme antécédents à l'adoption symbolique : l'utilité perçue et la facilité d'emploi perçue, souvent mobilisées pour l'intention comportementale d'usage (voir Agarwal et Karahanna 2000 ; Nah et al. 2004).

Notre approche du modèle d'AS varie sur ce point, selon nous il s'agit davantage d'**identifier** si l'innovation est une **« bonne idée »** (ou pas), avant de considérer les caractéristiques d'usage. En effet, Karahanna et Agarwal (2006) visaient à explorer l'adoption symbolique pour des utilisateurs d'une technologie pour laquelle ils n'ont pas nécessairement participé à la décision, et qui peut parfois même leur être imposée. En ce sens, Rawstorne et al. (1998 p. 324) précisent que dans un environnement d'adoption obligatoire, « l'adoption réelle n'a pas besoin d'être précédée nécessairement par l'adoption symbolique, tandis que dans un environnement d'adoption volontaire, l'adoption symbolique est pratiquement un prérequis pour l'adoption réelle ».

[24] Mérite d'effort : évaluation de l'utilisateur du retour sur les ressources dépensées pour pouvoir utiliser la technologie

[25] Enthousiasme intensifié : engagement avec lequel un utilisateur s'approche des comportements associés à l'utilisation

[26] TRA : Fishbein et Ajzen 1975

[27] TAM : Davis et al. (1989)

Ainsi, nous mobilisons le cadre d'AS dans son expression initiale, selon les trois étapes que sont la connaissance, le recueil d'information et l'évaluation, telles que nous les présentons circonstanciées ci-après.

Première étape d'adoption symbolique : la conscience de l'innovation

À notre connaissance, seuls Lesca et al. (2015) et Sapp et Korsching (2004) définissent l'étape de « conscience ». « The knowledge stage » est, selon Rogers (2003 p. 171), **le point de départ du processus** lorsqu'un « individu est exposé à l'existence d'une innovation et qu'il acquiert la connaissance sur son fonctionnement ». Sur la base des travaux de Rogers (1983), Sapp et Korsching (2004 p. 366) indiquent que l'« on ne peut pas traiter une innovation sauf sur la base de ce qui est **familier**, de ce qui est **connu** ». La définition de la connaissance de l'innovation de ces auteurs semble alors dépasser la seule « conscience », se mêlant avec l'étape de « renseignement ». En ce sens, Sapp et Korsching (2004) complètent leurs propos en introduisant la notion de complexité de la décision d'adoption, soit plus précisément la capacité pour les acteurs de distinguer la compatibilité et l'avantage relatif[28] de l'innovation. Si la complexité de l'innovation se définit comme « le degré avec lequel une innovation est perçue comme difficile à comprendre et à utiliser » (Rogers 2003 p. 16), Sapp et Korshing évoquent ici la difficulté de distinguer les notions d'avantage relatif et la compatibilité de l'innovation. Ils statuent alors que plus l'innovation apparait clairement aux adoptants potentiels, moins la technologie semble complexe, offrant alors plus de facilité à distinguer la compatibilité et l'avantage relatif de l'innovation (Sapp et Korsching 2004).

La littérature ne porte que peu d'explications sur l'étape de conscience. Les travaux traitant d'AS, et plus largement d'adoption d'innovation, énoncent la première étape du processus (« awareness ») sans préciser comment elle se constitue. Nous pouvons citer par exemple Hameed et al. (2012 p. 361) qui indiquent que « les chercheurs expliquent l'adoption d'innovation en termes de conscience, d'intérêt… » à l'appui des travaux de Fichman (2001) et Rai et al. (2009) dans lesquels le concept de « conscience »[29] n'est pourtant que très peu défini. Dans la littérature traitant d'AS, la définition de « conscience » semble inexistante (Karahanna et al .1999 ; Nah et al. 2004 ; Rawstorne et al. 1998 ; Sapp et Korsching 2004 ; Verra et al. 2012). Lesca et al. (2015), quant à eux, définissent l'étape de conscience comme « une prise de conscience » lorsqu'« un individu se rend compte de l'apparition d'une

[28] L'avantage relatif se définit comme « le degré avec lequel une innovation est perçue comme meilleure que l'idée qu'elle remplace » (Rogers 2003 p. 15)

[29] Rai et al. (2009 p. 270) précisent « Awareness : Key decision makers are aware of technologies ».

innovation ». Justement, Lesca et al. (2015 p. 43) énoncent la phase d'initiation du processus qui« consiste en des activités liées pour **reconnaître un besoin**, acquérir la connaissance ou la conscience ». Ce point mérite une attention particulière dans le déclenchement du processus d'adoption, et par conséquent de l'adoption symbolique de la SSI. En effet, si l'initiation du processus d'adoption consiste à reconnaitre une innovation pour répondre à un besoin (Hameed et al. 2012 ; Lesca et al. 2015), l'existence du besoin est alors fondamentale. Par conséquent, pour l'AS de la SSI, il s'agirait d'« acquérir la connaissance ou la conscience » **pour la SSI sur la base d'une besoin identifié**. Nous avons indiqué dans le chapitre SSI, dans un contexte « volontaire » que ce **besoin pouvait justement être lié à un risque** (Straub et Welke 1998) ou à une réponse isomorphique (Hu et al. 2007 ; McFadzean et al. 2007). En regard de notre problématique et questions de recherche, nous pourrons observer précisément la nature des influences sur cette étape, soit la reconnaissance de réponse à un besoin, le risque SI, soit l'innovation elle-même et donc la SSI.

Une fois la prise de conscience de l'innovation acquise par l'adoptant, il s'agit alors d'effectuer la phase de recueil d'information sur l'innovation.

Seconde étape d'adoption symbolique : renseignement sur l'innovation

Comme pour la première étape Sapp et Korsching (2004 p. 366), précisent que seule l'adoption « de ce qui est connu » peut être traitée. Pour Karahanna et al. (1999), le processus d'adoption symbolique peut se comparer avec la gestion du risque (au sens d'appréhender un objet inconnu et non pas au risque SI). Ces auteurs soulignent que l'incertitude liée au manque de connaissance de l'innovation peut conduire les potentiels adoptant à **accentuer leur communication sur l'innovation** (Karahanna et al. 1999). En effet, le besoin d'information pour « interpréter l'innovation et ses implications » nécessite, pour l'adoptant, d'accroitre ses interactions avec son environnement social qui peuvent alors impacter sa décision d'adoption **via l'influence informationnelle et normative** (Karahanna et al. 1999 p. 190)[30]. S'agissant de l'importance de la diffusion des informations sur l'innovation, Sapp et Korsching (2004) soulignent[31] que la **confiance accordée au réseau social** de l'adoptant serait plus importante que le contenu de l'information délivrée. Ils citent l'exemple du scepticisme à l'égard d'une nouvelle technologie qui résulterait de l'acquisition d'informations négatives par les potentiels adoptants. Ce scepticisme pourrait

[30] Sur la base des travaux de Rogers 1983

[31] Sur la base des travaux de Rogers 1995

être atténué par des informations délivrées par des sources éprouvées ou reconnues, vues par les potentiels adoptants comme n'ayant pas d'intérêt personnel significatif dans l'adoption ou dans le rejet de la nouvelle technologie (Rogers 2003). Karahanna et al. (1999 p. 190) indiquent qu'à cette influence informationnelle s'ajoute une « pression normative », conduisant le potentiel adoptant à réduire l'incertitude sur sa décision. En effet, disposant de la preuve de l'adoption par des pairs, le potentiel adoptant peut y voir une légitimité à prendre une décision similaire à ses pairs (Karahanna et al. 1999 p. 190). Ainsi, la visibilité, qui permet aussi de constater que l'innovation est utilisée par d'autres, peut contribuer au recueil d'information en ce sens où le potentiel adoptant dispose davantage d'information sur une innovation en situation d'exploitation (Karahanna et al. 1999).

Klonglan et Coward (1970 p. 81) étayent précisément l'effet de l'influence sociale sur le potentiel adoptant, en pointant le « rejet symbolique » dans la situation suivante :

- à l'instant T1, un individu A a adopté l'usage de l'innovation alors que l'individu B est dans la phase d'adoption symbolique
- à l'instant T2, A abandonne l'innovation et cette information est transmise à B
- à l'instant T3, B peut rejeter l'innovation avant de l'utiliser (rejet symbolique).

Dans cet exemple, l'influence de l'information délivrée à B apparait clairement sur le rejet symbolique lors de l'étape « recueil d'information sur l'innovation ». Klonglan et Coward (1970) ne précisent pas les raisons du rejet, qui selon nous et dans ce cas, pourraient être liées au « scepticisme » (Sapp et Korsching 2004) ou aux normes subjectives de B quant à l'adoption (Karahanna et al. 1999). Dans le deuxième cas, ces résultats sont concordants avec les travaux de Karahanna et al. (1999) qui soutiennent l'influence majeure des **normes subjectives** pour l'AS (soit la façon dont sera observée la décision du potentiel adoptant par les membres de son réseau d'influence), alors que cette influence est moins prégnante pour l'adoption d'usage.

Cependant, contrairement au modèle de processus d'AS, Klonglan et Coward (1970) ne précisent pas si l'adoptant effectue la phase suivante d'évaluation pour rejeter symboliquement l'innovation. Nous faisons l'hypothèse que l'étape d'information est suffisante pour rejeter symboliquement l'innovation, donnant alors tout son sens à l'influence sociale énoncée dans la littérature (Klonglan et Coward 1970 ; Sapp et Korsching 2004).

L'adoptant potentiel disposant d'informations suffisantes sur l'innovation doit alors mesurer la possible adaptation en réponse à son besoin, ce qu'il réalise dans la phase suivante, « l'évaluation de l'innovation ».

Troisième étape d'adoption symbolique : l'évaluation de l'innovation

Klonglan et Coward (1970 p. 79) précisent l'étape d'évaluation comme « une étape où l'adoptant **applique de façon abstraite** l'innovation à sa **situation particulière** pour décider si **l'adoption est adaptée** ou non ». Il s'agit, sur la base des caractéristiques obtenues lors de la phase d'information, de tester l'innovation en regard des spécificités du besoin perçu par l'adoptant. En ce sens, Sapp et Korsching (2004) soulignent l'importance de l'avantage relatif et de la compatibilité perçus de l'innovation. Selon ces auteurs, l'avantage relatif et la compatibilité peuvent contribuer à l'explication de l'AS même si elles sont davantage prégnantes dans l'adoption d'usage (Sapp et Korsching 2004).

Sapp et Korsching (2004 p. 352) considèrent l'AS comme « constituée par la façon dont les individus répondent aux messages, à la persuasion sociale et aux attentes normatives qu'ils perçoivent ». Ils définissent précisément le cadre d'AS avec ses déterminants : **l'avantage relatif** (l'innovation portant un intérêt supérieur à l'idée qu'elle remplace), la **compatibilité** (l'innovation est perçue comme compatible avec les valeurs, les expériences et les besoins de l'adoptant potentiel), la **complexité** (difficulté perçue à comprendre et éventuellement utilisée l'innovation), et enfin **l'essayabilité** (l'innovation peut être expérimentée et observée). Notons que certaines de ces caractéristiques sont complémentaires à celles développées par Karahanna et al. (1999) qui évoquent pour le processus d'AS des caractéristiques que les potentiels adoptant pourraient enrichir par : la perception d'utilité, la facilité d'utilisation, la démontrabilité de résultat, la visibilité et l'essayabilité. Ils notent que l'adoption serait seulement basée sur l'instrumentalité d'utilité et la perception d'image. En ce sens, Nah et al. (2004) soulignent le parallèle entre les résultats de Karahanna et al. (1999) et deux constructions importantes de TAM, soit l'utilité perçu et la facilité d'emploi perçue. À l'appui des résultats empiriques de Karahanna et al. (1999), Nah et al. (2004) font l'hypothèse que l'utilité et la facilité d'emploi perçus peuvent avoir des effets directs sur l'AS.

Les résultats des travaux Karahanna et al. (1999 p. 200) les conduisent à souligner que l'essayabilité et la visibilité de l'innovation contribuent à l'AS. Selon eux, l'essayabilité, soit la possibilité de tester l'innovation pour répondre au besoin du potentiel adoptant, est plus pertinente pour l'adoption symbolique que pour l'adoption d'usage. La visibilité, quant à elle,

contribue, à l'exploration de l'innovation et permet au potentiel adoptant, de disposer d'un volume accru d'informations permettant sa mise en application abstraite. À ces deux caractéristiques s'ajoute la visibilité, qui permet aussi de constater que l'innovation est utilisée par d'autres (Karahanna et al. 1999). En synthèse, l'essayabilité et la visibilité sont des caractéristiques importantes de l'innovation en ce sens où elles permettent « la **réduction du risque et de l'incertitude** des conséquences attendues par l'utilisation de l'innovation » (Karahanna et al. 1999). Ces auteurs appuient leur commentaire sur l'importance fortement réduite, après l'adoption, de l'essayabilité, de la démontrabilité, de la facilité d'emploi et de la visibilité, renforçant leur hypothèse que ces caractéristiques seraient plus importantes pour l'AS.

Auteurs	Adoption Symbolique	Adoption d'usage
Klonglan et Coward (1970)	Répondre à un besoin Information sur l'innovation Normes subjectives	Essayabilité Adaptation au besoin
Rawstorne et al. (1998)	Avantage relatif Compatibilité Complexité Essayabilité Normes sociales	/
Karahanna et al. (1999)	Utilité perçue Facilité d'usage Démonstrabilité du résultat Visibilité Essayabilité	Usage Exploration
Sapp et Korsching (2004)	Réponses émotionnelles et affectives aux messages Persuasion sociale et croyances normatives perçues	Disponibilité Essayabilité Ressources financières Assistance technique »

Tableau 3 : Synthèse des concepts mobilisés dans la littérature d'adoption symbolique

Attendu que l'objet de notre recherche n'est pas de tester le modèle d'AS, ni ses déclinaisons, nous la mobilisons uniquement pour dissocier les différentes étapes qui conduisent à l'acceptation « symbolique » de la SSI. À ce stade de nos travaux, nous n'écartons pas les

concepts développés par les auteurs qui ont adapté, pour leur objet de recherche, des cadres théoriques basés sur l'adoption symbolique.

Les trois étapes de l'AS ayant été décrites en regard du modèle d'AS initial de Klonglan et Coward (1970) nous pouvons dès lors préciser davantage la notion de décalage entre les phases d'adoption symbolique et d'adoption d'usage.

Décalage entre la phase d'adoption symbolique et la phase d'adoption d'usage

En s'appuyant sur la **latence entre adoption symbolique et adoption d'usage**, le modèle d'AS peut permettre d'expliquer l'adoption ou le rejet. Ce point de « bascule » entre adoption et rejet (Sapp et Korsching 2004) doit s'observer en complétant les facteurs sociologiques ou économiques par des facteurs externes au potentiel adoptant. Ainsi, l'adoption incomplète décrit une situation où l'individu est tout à fait favorable à l'utilisation d'une innovation, résultant à l'adoption symbolique (phase A), mais des facteurs structurels contraignent le passage à la phase d'usage (phase B) (Klonglan et Coward 1970). Deux formes d'adoption incomplète sont « l'adoption contrainte » et « l'adoption anticipée ». La forme d'adoption contrainte survient, par exemple, lorsqu'un individu est favorable à l'utilisation de transports en commun, mais il n'est pas possible matériellement de les utiliser car il n'existe pas encore de système valable de bus ou de train. L'adoption anticipée est une forme d'adoption incomplète à cause de la nature de l'innovation. La forme d'adoption anticipée survient, par exemple, lorsqu'un individu a décidé la construction d'un abri anti-atomique, mais ne l'a pas réalisé « parce qu'il n'y a aucun besoin de l'utiliser » (Klonglan et Coward 1970 p. 80). Pour Rawstorne et al. (1998), la **dissonance d'innovation** est un terme que Karahanna a emprunté à Rogers (1995) pour renvoyer à une situation dans laquelle l'adoption symbolique est en désaccord avec l'adoption réelle. Par exemple, dans un environnement d'adoption obligatoire, un utilisateur final potentiel peut être peu enclin à utiliser un SI tout en étant contraint à son usage. Karahanna et Agarwal (2006 p. 6) présentent un exemple circonstancié de l'adoption contrainte dans le « cas d'une demande de service client automatisée conçue pour un vendeur ». Le vendeur considère que cette demande automatisée « n'est pas une bonne idée parce qu'elle réduit ou élimine l'interaction de face à face avec le client ». Le vendeur utilisera cette innovation car elle lui est imposée alors que **le processus d'AS a conduit à un rejet**. Alors que Karahanna et Agarwal (2006) ont utilisé l'AS justement pour mesurer l'acceptation mentale volontaire, cet

exemple leur permet d'étayer qu'une adoption symbolique (en tant que résultat d'adoption) n'est pas nécessaire dans un contexte contraint.

Présentées de façon différente et telles qu'illustrées dans la figure 9, l'adoption effective de l'idée peut être suivie de l'adoption ou du rejet de l'innovation matérielle. Pour donner une perspective à l'adoption symbolique, **en tant que résultat**, nous pouvons citer un exemple de concept adopté et de matérialité rejetée. Ainsi, un manager en responsabilité des SI de son organisation est informé de la mise sur le marché d'une technologie innovante, permettant de renforcer la disponibilité de ses infrastructures. À ce stade du processus d'adoption, il s'agirait alors d'une adoption symbolique, le manager étant convaincu des avantages de l'innovation. Toutefois, le manager pourrait ne pas vouloir mettre en œuvre cette nouvelle technologie car des investissements conséquents ont été réalisés récemment pour la disponibilité de son SI. Nous comprenons aisément dans cet exemple pourquoi il est nécessaire de **considérer indépendamment les deux phases** pour aborder globalement la décision du manager. Cet exemple s'inscrit dans la perspective des propos de Klonglan et Coward (1970), soulignant que les influences sur l'adoptant sont prégnantes pour expliquer l'adoption initiale alors que les influences matérielles, composées de facteurs structurels, expliquent davantage l'adoption d'usage. À l'inverse, n'observer que la décision finale, soit dans l'exemple ci-avant un rejet d'usage, ne permettrait pas la distinction entre les raisons du rejet de l'innovation, qu'elle soit liée aux aspects économiques ou que ce soit une « mauvaise » innovation.

Ainsi l'AS a établi deux phases explicites dans l'adoption : l'acceptation d'une idée et utilise ensuite l'adoption, « indépendamment de si l'innovation adoptée est matérielle ou immatérielle ». Le modèle à deux phases facilite l'identification de décalage d'adoption dans le temps et permet l'étude explicative des influences sur chaque phase.

Si le processus d'adoption symbolique permet de considérer la succession d'étapes pour conduire à l'adoption symbolique, il est aussi pertinent pour étudier de quelle façon ces étapes conduisent à l'adoption ou, le cas échéant, au rejet symbolique. La littérature énonce des contextes dans lesquels les étapes peuvent ou ne peuvent se succéder. Nous traitons dans le paragraphe suivant l'adoption ou rejet symbolique en tant que résultat du processus d'adoption symbolique.

Adoption ou rejet symbolique

Si pour Verra et al. (2012 p. 8) l'adoption symbolique est « un processus d'évaluation mentale et affective d'un nouveau système », sans que le concept d'affect ne soit précisé dans leurs travaux. Ces mêmes auteurs livrent toutefois un éclairage intéressant sur l'adoption symbolique en indiquant qu'il s'agit, pour le potentiel adoptant, de savoir ce que va symboliser cette technologie » (Verra et al. 2012 p. 8). Ils précisent qu'il s'agit d'un concept issu des travaux de Feldman et March (1981) sur le « signal et symbole ». L'adoption symbolique rejoindrait, selon eux, le management de l'information et l'utilisation des SI dans l'organisation pour assoir symboliquement la légitimité de la décision (la décision d'adoption du SI, en l'occurrence, permettrait d'envoyer un signal aux acteurs, démontrant que l'organisation est correctement gérée, Verra et al. 2012). Notons que Sapp et Korsching (2004 p. 352) indiquent justement que l'AS est une « réponse affective aux messages cognitifs de l'innovation et de la persuasion sociale de leaders d'opinion » et par conséquent, l'AS représente l'**attitude du potentiel adoptant**.

Dans la perspective de nos travaux sur la SSI, ce point renforce, selon nous, la nécessité pour les top-managers de décider l'adoption de la SSI (Hu et al. 2007 ; Kankanhalli 2003 ; Knapp et al. 2006 ; Straub et Welke 1998). En effet, selon le principe de Verra et al. (2012), cette décision, au-delà de la nécessité de protéger les SI, permettrait aux top-managers « d'envoyer un signal aux acteurs » pour indiquer que les décisions sont correctement prises dans l'organisation et aussi d'influer alors directement sur la culture sécurité dans l'organisation (Barlette et Fomin 2010 ; Knapp et al. 2006 ; Siponen 2000).

Après avoir détaillé les trois étapes d'AS et les concepts sous-jacents de chacune, puis les principes de passage d'une phase à l'autre, nous pouvons présenter une synthèse de ce cadre théorique sur la base de l'étude de Lesca et al. (2015) pour la pré-adoption des SI (cf. Tableau 4), que nous avons restreinte aux individus, en écartant l'implémentation de l'innovation par les organisations afin de respecter notre objet de recherche.

Auteurs	Pré-adoption		
Klonglan et Coward (1970)	**Prise de conscience** Un individu se rend compte de l'apparition d'une innovation.	**Renseignement** L'individu explore activement des informations sur l'innovation.	**Évaluation** L'individu évalue si l'innovation est adaptée à ses besoins (adoption symbolique).
Rogers (2003)	**Connaissance** Exposition à l'innovation et à la façon dont elle fonctionne.		**Persuasion** Une attitude favorable ou défavorable est formée vers l'innovation.
Fichman (2001) ; Rai et al. (2009)	**Prise de conscience** Les principaux décideurs apprennent l'existence d'une nouvelle IT.		**Intérêt** L'organisation cherche à en savoir plus sur la nouvelle IT.
Hameed et al. (2012)	**Initiation** Reconnaissance d'une innovation IT qui peut répondre à un besoin, l'acquisition des informations concernant l'innovation IT, et le positionnement à propos de l'adoption de l'innovation.		

Tableau 4 : Synthèse des processus de pré-adoption dans la littérature SI

(adapté de Lesca et al. 2015 p 42)

3.1.3. Intérêt du modèle d'AS pour nos travaux

Selon Rogers (2003), le processus de décision d'adoption d'innovation conduisant à l'usage peut être conceptualisé comme un passage de la connaissance initiale d'une innovation, à l'acceptation ou au rejet de cette innovation. Karahanna et al. (1999) mobilisent le cadre d'adoption symbolique car ils précisent qu'un ensemble de caractéristiques, considéré par le potentiel adoptant, jalonnent le processus de décision avant de conduire à l'adoption ou au rejet symbolique. Pour Karahanna et al. (1999 p. 185), les « constructions clés dans ce processus de décision d'adoption d'innovation sont les caractéristiques perçues de l'innovation, l'attitude et les croyances de l'individu et les communications reçues pour l'innovation dans l'environnement social de l'individu ».

Le cadre théorique d'AS peut permettre l'étude des facteurs d'adoption pour la théorie et pour la pratique. Par exemple, Karahanna et al. (1999 p. 184) ont mobilisé le cadre d'AS et précisent, pour l'adoption d'un nouveau SI, que d'identifier les « déterminants des antécédents d'adoption » et la façon dont ils diffèrent, peut éclairer « notre état actuel de

connaissance ». Selon nous la littérature est relativement silencieuse sur les fondements de la décision spécifique à l'adoption de la SSI. Dans une perspective pratique, le cadre d'AS peut permettre d'observer les influences majeures et leurs interactions dans la décision d'adopter (ou de rejeter symboliquement) la SSI. De façon comparable, Karahanna et al. (1999) ont utilisé l'AS justement pour pointer les caractéristiques pertinentes lors du processus d'adoption, de façon à améliorer la prise en compte de l'innovation dans chaque étape. Précisément, le modèle d'adoption de Klonglan et Coward (1970) permet d'aborder conceptuellement l'AS comme un point de décalage dans le processus d'adoption, soit **les influences qui permettront de passer de l'idée à la pratique**. En ce sens, le cadre d'AS met en perspective méthodologiquement les étapes comme des caractéristiques indépendantes mais observées globalement pour en comprendre les interactions.

Ensuite, les variables sociologiques sont plus prégnantes pour l'explication de l'adoption symbolique, les variables économiques sont relativement plus importantes pour l'explication de l'adoption d'utilisation (Klonglan et Coward 1970). Par exemple, pour Sapp et Korsching (2004) le modèle d'AS répond à un besoin académique des « sciences humaines qui examinent aussi des **processus de prise de décisions** de citoyen pour des technologies controversées ». Ils précisent, dans ce cadre de recherche, que les résultats empiriques font **« majoritairement émerger les effets de l'information positive et négative acquise » au travers des médias et des éléments de langage**. En effet, à l'appui des travaux de (Slovic 1999), l'évaluation du risque pour une nouvelle technologie relève de la maitrise de la **communication sur la complexité** de cette technologie. En ce sens, le cadre d'AS permet l'étude de ces influences, qui semblent interagir lorsqu'il s'agit de décision sur une idée ou un concept peu connu.

Aussi, selon Klonglan et Coward (1970) si les influences sociologiques sont prégnantes pour l'adoption de l'idée et les facteurs économique plus importants lorsqu'il s'agit de la mise en pratique, nous comprenons aisément les liens possibles entre ces deux phases. Ainsi, l'articulation des influences sociologiques et économiques pourraient être complémentaires afin de comprendre, dans un temps ultérieur, la mise en œuvre de la décision.

Enfin, le cadre d'AS peut porter un éclairage sur les décisions de rejet ou les **décisions d'adoption incomplète de la SSI**, soit les raisons qui ont « empêché » le passage d'une phase d'adoption symbolique à une phase d'adoption matérielle.

Nous rappelons que, selon Klonglan et Coward (1970), l'adoption symbolique relève de l'adoption initiale de l'idée ou du concept alors que les facteurs structurels expliquent davantage l'adoption d'usage. En ce sens, le modèle d'adoption symbolique apparait comme un cadre théorique adapté à nos objectifs, car, justement, il permet **de centrer notre étude en amont de la mise en œuvre**, qui relève de la deuxième phase du processus d'adoption. Précisément, l'AS permet d'observer la possible prise en compte d'un besoin potentiel de protéger le SI d'une part. D'autre part, l'AS permet d'observer les influences internes et externes sur la décision, qu'il s'agisse potentiellement de la prise en compte des risques, de la compétence nécessaire pour adopter symboliquement la SSI ou encore de situer la SSI par rapport aux pratiques du réseau d'influence du potentiel adoptant[32]. Enfin, l'AS offre la possibilité d'étudier comment est évalué la SSI en regard de son adaptation à ce besoin, indépendamment de la phase de mise en œuvre et de ses considérations pratiques.

3.2. Perception des risques

À notre connaissance, dans le champ de la SSI, seuls huit travaux (cf. « 3.2.7 Perception des risques et SSI » p. 165) ont pour **objectif d'explorer le risque SI perçu**, ce qui présente la connaissance académique sur la **perception des risques et la décision pour la sécurité des SI** (Albrechtsen 2007 ; Albrechtsen et Hovden 2009 ; Loch et al. 1992 ; Straub et Welke 1998 ; Huang et al. 2010 ; McFadzean et al. 2007 ; Taylor et al. 2006 ; Tsohou et al. 2006). Si nous avons élargi de champ de la revue de la littérature sur le « risque » afin d'en distinguer tous les concepts, nous centrons notre étude sur la perception des risques. En ce sens, pour Slovic et al. (1984 p. 183), dont les travaux sont fondateurs pour la perception des risques, « la recherche dans le cadre de la théorie de décision comportementale peut **contribuer à bien des égards à la gestion et à la régulation du risque** ». Avant de présenter les concepts sous-jacents la perception des risques, nous définirons le risque et les différents points de vue des auteurs sur cette notion avant de détailler les approches théoriques (paradigmes) dans lesquels les risques sont étudiés, ainsi que les biais d'évaluation des risques. Ensuite nous présenterons les huit travaux académiques traitant de la perception des risques SI, à la lumière de la littérature sur les risques, développée notamment par Fischoff et al. 1978 et Slovic et al. (1978 ; 1982 ; 1984).

[32] Sapp et Korsching (2004 p. 354) évoquent « l'influence des référents importants ».

3.2.1. Définition du risque

Selon Yates et Stones (1992) il n'est pas surprenant d'observer autant de définitions du risque que de publications académiques sur le sujet. Pour Peretti-Watel (2003 p. 2) et Kermisch (2011), l'étymologie du mot risque prend son origine à risco (italien) ou à riesgo (espagnol) qui signifie l'écueil qui menace les navires ou le « récif », comprenant à la fois **l'évènement périlleux** et les **dommages** liés à cet **évènement**. Fischoff et al. (1981 p. 2) définissent le risque comme **l'existence d'une menace**. Ainsi, « les individus qui utilisent le mot risque de différentes façons, renvoient aux entités qui n'ont aucun lien l'une avec l'autre » (Yates et Stones 1992 p. 2). Par exemple, pour une technologie, si les profanes et les spécialistes des risques de cette technologie utilisent le terme « risque » différemment, ils peuvent convenir des faits spécifiques tout en étant en désaccord avec le niveau de risque.

Précisément, pour Cadet et Kouabénan (2005) si les différences d'appréciation des risques relèvent davantage de la recherche d'un **niveau commun de risque**, soit une « estimation quantitative susceptible de constituer une référence commune sur des activités que tous s'accordent à considérer comme risquées ». Pour ces mêmes auteurs, la difficulté de s'accorder sur ce niveau commun repose sur les caractéristiques propres au risque qui dans le même temps expose les champs cognitifs des évaluateurs à des informations concordantes et discordantes.

Ceci éclaire l'ambiguïté et la complexité de la notion de risque. D'une part le risque « est toujours potentiel et virtuel car, **lorsqu'un risque se matérialise**, il ne s'agit plus d'un risque mais d'un **sinistre** » (Kermisch 2012 p. 1). D'autre part, selon cette même auteure, du point de vue épistémologique, le risque est « complexe à circonscrire dans la mesure où le savoir à propos du risque est un "savoir à propos d'un non-savoir" ». Plus globalement, le risque se définit dans la discipline de recherche en psychologie (Amalberti 1996 ; Hermand et Chauvin 2008 ; Cadet et Kouabénan 2005 ; Slovic et al. 2004 ; Sjöberg et al. 2004) et en SI (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Dhillon et Torkzadeh 2006), comme la **probabilité** d'un évènement indésirable et l'ampleur de ses **conséquences**. Cette conception du risque constitue la base des modèles de risque nommé paradigme de **l'utilité espérée** (ou encore normatif probabiliste) et le **paradigme cognitif**[33]. Elle prend naissance dans le champ financier et économique au XIVème siècle pour traiter les évaluations des accidents maritimes.

[33] Les trois paradigmes d'étude du risque sont : 1) l'utilité espérée, 2) cognitif et 3) psychométrique (Cadet et Kouabénan 2005)

Sjöberg et al. (2004) s'appuie sur les travaux de Short (1984) pour définir le risque comme la probabilité qu'un individu expérimente **les effets d'un danger**. Sémantiquement, la notion de risque est souvent assimilée à un danger ou à une menace, accentuant davantage « l'existence d'aspects subjectifs » (Cadet et Kouabenan 2005 p. 9). En effet, la plupart des humains sont confrontés quotidiennement à des événements **dangereux,** conduisant à s'interroger sur leurs **perceptions du risque**. En ce sens, il convient que l'individu identifie préalablement la situation comme « risquée », avant d'entreprendre l'évaluation du niveau de risque. Nous **écartons toutefois la notion de danger** à l'appui des travaux de Magne (2010). Selon ce dernier, « le danger ne possède pas un caractère potentiel comme le risque, mais une capacité **intrinsèque** et **certaine** de produire des dommages ». Par exemple, il évoque le danger pour un homme de s'approcher d'un ours, alors qu'en cage, le potentiel de dommage n'a plus de réalité (Magne 2010 p. 20). Si le danger est une source potentielle de dommage, nous l'assimilons à une menace, à laquelle l'évaluateur peut être exposé. Le danger ou menace se traduit en risque **dès lors que l'évaluateur y est confronté** (Magne 2010).

Cette conception probabiliste s'inscrit dans le projet d'évaluer quantitativement le risque le plus objectivement possible dont seul « un nombre important d'observations empiriques » permettrait alors de qualifier le risque « d'objectif » (Kermisch 2012 p. 3). Ainsi, ce modèle du risque est critiqué comme partiellement inadapté par Sowby (1965) et Starr (1969)[34] bien que majoritairement utilisé par les « experts » (Hermand et Chauvin 2008 ; Kermisch 2012 ; Slovic et al. 1984). En effet, un risque, pour lequel peu ou pas de données significatives objectives sont disponibles, ne peut s'évaluer selon un calcul probabiliste de survenance et d'impact (Slovic 1979). Ceci permet à Slovic et al. (1982a) d'inscrire le risque comme un objet social attendu qu'il n'est perçu que par ses évaluateurs et en regard de déterminants sociaux. Pour préciser ce constat, Cadet et Kouabénan (2005 p. 18) précisent que le risque n'est pas seulement un concept caractérisant un danger pouvant provenir d'une technologie ou de l'environnement mais « aussi une valeur où figurent des choix sociaux ». En ce sens, Yates et Stone (1992) soulignent la divergence des catégories[35] de résultats prises en compte pour un même risque et Slovic et al. (1978 ; 1984) précisent que les individus considèrent seulement une partie des caractéristiques du risque. Pour illustrer

[34] Les travaux de Sowby (1965) et Starr (1969) sont pionniers sur les risques technologiques

[35] Nous développons ci-après la notion de catégorie de Yates et Stone (1992) et Slovic et al. (1984). Notons toutefois que les catégories sont situationnelles et permettent d'identifier les gains et pertes liés à un risque, alors que les caractéristiques du risque sont définies par 16 items tels que par exemple la volonté de s'exposer au risque, le contrôle possible sur le risque, la familiarité de la situation à risque, la nouveauté du risque ou encore la fatalité des conséquences…

cette limite, Sowby (1965) a constaté la faible acceptation du public de risques quantitativement moins élevés que d'autres. Par exemple, une illustration de ce principe considère trois activités : fumer du tabac, conduire une voiture et habiter près d'une centrale nucléaire. Selon Sowby (1965), si les personnes fument et conduisent, pourquoi n'habitent-t-elles pas près d'une centrale nucléaire qui est une activité « probablement » moins risquée (Sjöberg et al. 2004) ? Une autre illustration de cette limite est établie par Starr (1969) qui critique l'approche probabiliste de Sowby (1965). Il démontre la **notion d'acceptation**, dans laquelle les individus associent à l'évaluation du risque, certes les conséquences négatives mais aussi leur **avantage**, conduisant alors à l'acceptation de l'activité à risque, ce qui sera plus tard qualifié de « volontarisme » pour le risque (Slovic et al. 1982) et mettant en perspective « le bénéfice ».

Cette critique sur l'étude du risque, réduite à la probabilité et les conséquences, est synthétisée par Cadet et Kouabénan (2005) et Hermand et Chauvin (2008) qui indiquent l'hétérogénéité de la nature et des conséquences des risques, rendant difficile une évaluation quantitative commune. Cette synthèse résume l'origine des travaux de Slovic et al. (1979 ; 1982 ; 1987) sur le **paradigme psychométrique**. Ces auteurs précisent que « si le danger est réel, le **risque est socialement construit** » et ajoutent que « l'évaluation de risque est en soi subjective et représente un mélange de science et de jugement avec des facteurs psychologiques, sociaux, culturels et politiques importants » (Slovic 1999 p. 689). Pour Kermisch (2012 p. 5), ce point éclaire une conception **constructiviste du risque**, précisant à la fois l'influence socioculturelle, avec laquelle les individus définissent le risque, et **la notion subjective**, au sens littéral de « propre à un sujet », où le risque « n'est pas considéré comme quelque chose d'extérieur que l'on peut percevoir » **indépendamment de son contexte**, pour les individus comme pour les organisations. En ce sens, pour les organisations, l'évaluation du risque consiste à déterminer l'exposition au risque de pertes, identifier les pertes potentielles et définir la probabilité de survenance de ce risque (Yates et Stone 1992). Dans cette définition étendue, deux concepts clés du risque sont la probabilité et l'effet, où le risque consiste en une combinaison de probabilité de perte et de signification de perte**, afin de permettre une décision** (Yates et Stone 1992 ; Mitchell 1995). Précisément, la décision relève d'un choix qui vise à atteindre un résultat *a minima* aussi satisfaisant que celui du plus faible résultat prévu ou possible. Lorsque le résultat est atteint, la décision est alors réussie, à l'inverse une perte est un échec de décision (Yates et Stone 1992). « Ainsi un problème de décision est le défi de prendre des décisions réussies » dont le risque de perte est seulement un des résultats possibles (Yates et Stone 1992 p. 8). Notons

que la notion de décision est sous-tendue dans la définition de la SSI de Solms (2006 p. 166) soit les dispositions à définir et mettre en œuvre dans « la discipline pour atténuer les risques ayant un impact sur la confidentialité, l'intégrité et la disponibilité des ressources informatiques », activité alors pertinente pour répondre aux exigences de gouvernance d'entreprise.

Si les trois paradigmes, utilité espérée, cognitif et psychométrique, n'ont pas les mêmes propriétés, définies en détail ci-après, ils s'inscrivent toutefois dans les théories **comportementales de la décision**. En effet, Cadet et Kouabenan (2005 p. 9) soulignent le lien entre risque et gestion du risque, qui pourrait conduire, pour le risque étudié, à une perte potentielle attendue suite à une prise de décision. Pour ces trois paradigmes, il s'agit alors d'étudier les risques perçus (ou évalués dans le cas du paradigme « normatif probabiliste ») dans une perspective à visée comportementale et ainsi d'observer les **réactions des individus** face au risque pour comprendre alors **les décisions**. Pour cette raison, Kermisch (2012) réconcilie les trois paradigmes car, selon elle, ils visent le même objet. D'une part, la conjonction de leur conception, individuelle et socioculturelle, enrichit l'étude et la compréhension pour appréhender le risque. D'autre part, la discipline de gestion du risque offre un « outil conceptuel riche » selon une définition multidimensionnelle du risque : la « composante quantitative chiffre le potentiel de dommages, alors que la composante constructiviste rend compte du risque compris comme représentation des **inquiétudes individuelles** et collectives » (Kermisch 2012 p. 7).

Nous concluons la définition du risque par la vision globalisante « plus structurale et fonctionnelle » de Cadet et Kouabenan (2005 p. 11), qui identifient les concepts sous-jacents de l'évaluation d'une situation à risque et que nous synthétisons par :

- **plusieurs informations et sources d'informations** à analyser simultanément ou successivement. **Aucune information isolée** « ne fournit une description satisfaisante de la situation » (Cadet et Kouabenan 2005 p. 11).
- les **incertitudes** multidimensionnelles. D'une part, les « signes ou indices utilisés pour caractériser le risque » n'ont pas de sens univoque D'autre part, les catégories de risque considérées[36] ne sont pas nécessairement exhaustives et comparable d'un individu profane à l'autre pour un même risque (Yates et Stone 1992). Enfin

[36] Les catégories de risques sont conceptuellement définies par Yates et Stones 1992, nous les décrivons dans la section « Le risque acceptable » p. 118

l'incertitude est intrinsèquement liée à l'évolution de la situation étudiée. Il s'agit de faire « des pronostics en présence d'incertitude à partir des informations présentes » (Cadet et Kouabenan 2005 p. 11).

– **les bénéfices attendus.** Nous comprenons aisément, que le risque n'est admissible lorsque les enjeux visés, ou les avantages perçus, dépassent les pertes perçues (Slovic et al. 2004).

Ces facteurs sont illustrés dans une planche de Gary Trudeau et présentée par Slovic et al. (2004, cf. Figure10).

Afin d'appréhender la façon dont se combinent ces facteurs pour évaluer le risque, nous pouvons observer les trois paradigmes d'étude du risque. Toutefois, en préambule il convient de définir davantage les concepts et heuristiques mobilisés lors de l'évaluation du risque.



Figure 10 : Street calculus

G Trudeau (1994) cité par Slovic et al. (2004)

3.2.2. Concepts de l'étude des risques

Yates et Stone (1992) indiquent que la seule finalité de l'évaluation du risque est de savoir **si un risque est acceptable**. Si pour Sjöberg et al. (2004 p. 8) la **perception des risques** est **l'évaluation subjective** de la probabilité qu'un type spécifique d'accident survienne et de quelle façon les conséquences concernent l'évaluateur, il convient de caractériser les facteurs pris en compte dans cette évaluation. Ainsi, ce constat rejoint celui de Slovic (1999 p. 689) qui précise que « le risque est socialement construit ». Ce sont alors les concepts du risque que nous définissons ci-après, dans le projet d'aborder comment ils sont mobilisés dans les trois paradigmes de risques et d'en étudier leur biais. Ces concepts sont présentés selon la définition du risque avec l'incertitude, les conséquences et enfin le risque acceptable.

L'incertitude

L'incertitude est, sinon le premier, le concept clé du risque, définissant la réalité de l'évènement et sa **possibilité de survenance**. Pour plusieurs auteurs (Hermand et Chauvin 2008 ; Douglas et Wildavsky 1983 ; Peretti-Watel 2003), l'incertitude est une composante intrinsèque du risque, car « si tous cherchent à gérer le risque, tous savent que s'ils avaient des certitudes, ils n'auraient pas à faire au risque » (Sjöberg et al. 2004p. 7). Il s'agit aussi d'une construction psychologique qui n'existe seulement dans l'esprit car si la connaissance d'une personne était complète, cette personne n'aurait aucune incertitude » (Sjöberg et al. 2004). Yates et Stone (1992) précisent que le risque n'est pas un objectif du décideur mais qu'il s'impose à lui comme une **alternative incertaine** qu'il considère **subjectivement**. En ce sens, l'incertitude est liée à de nombreuses théories comportementale et psychologique, agissant comme médiateur des décisions en environnement incertain. Ainsi, la **réalité même du risque est incertaine**, car dépendante d'un résultat qui est attendu comme incertain par le décideur. En d'autres termes, ce qui est considéré comme perte pour un individu peut ne pas l'être pour un autre et la probabilité de perte sera définie différemment de l'un à l'autre.

L'incertitude peut aussi prendre forme dans **l'exhaustivité des catégories** considérées. Pour illustrer ce principe, citons l'exemple de changement d'emploi d'un individu, en l'occurrence *« Jane Smith »* selon Yates et Stone (1992). Celle-ci définit ses attentes pour son futur emploi, indiquant la localisation, le salaire et la nature des tâches confiées, comme catégories principales. Si Jane Smith choisi un emploi A, il n'est pas certain que ses futurs

collègues de travail ne soient pas une source d'inconfort. L'exemple de Yates et Stone précise que si Jane Smith avait considéré cette catégorie, elle n'aurait sans doute pas pris l'emploi A. Ces auteurs renforcent **l'incertitude de catégorie**, car parfois c'est le risque lui-même qui limite les catégories accessibles par les « profanes », par exemple lorsqu'il s'agit de nouvelle technologie. Par définition, l'absence de connaissance sur une nouvelle technologie, **limite les catégories activables car la nature des pertes possibles est inconnue** du grand public (Slovic et al. 1985). Enfin, l'incertitude de catégorie peut prendre forme dans la **naïveté** même de l'individu, que Yates et Stone (1992 p. 12) illustrent par le risque d'être contaminée par le SIDA, « maladie mortelle et incurable » à cause « de son activité sexuelle, de prise de drogue ou encore de transfusion sanguine ».

Notons que l'incertitude est un concept mobilisé par plusieurs auteurs pour la gestion du risque SI (Bandyopadhyay et al. 1999 ; Karahanna et al. 1999). Karahanna et al. (1999) ont réalisé une adaptation du cadre d'adoption symbolique, pour les évaluations d'une innovation technologie, par les potentiels adoptants. Ces auteurs précisent que les individus, **en défaut de connaissances** spécifiques sur la nouvelle technologie, vont mobiliser un large ensemble de caractéristiques afin de forger leur décision. Notamment, l'essayabilité et la visibilité de l'innovation contribuent à l'adoption symbolique car elles sont « importantes dans la réduction du risque et l'incertitude des conséquences attendues d'utiliser l'innovation » (Karahanna et al. 1999 p. 200). Si l'objectif, dans ce contexte précis de décision, n'est pas d'arbitrer le risque, nous pouvons toutefois établir un parallèle entre la compensation de l'incertitude par l'essayabilité et la visibilité, en tant qu'apport d'informations pouvant *in fine* limiter un résultat défavorable. Alors que Yates et Stones (1992) définissent la décision pour le risque comme un choix parmi plusieurs alternatives, justement afin d'atteindre un objectif satisfaisant, les évaluations des top-managers « ne tiennent généralement pas compte des évaluations de probabilité précises » (Bandyopadhyay et al. 1999 p. 440). Précisément, selon ces auteurs, les top-managers traitent leur décision pour le risque sur le volume de conséquences négatives principalement, en **écartant l'incertitude de survenance de ce risque**.

Les conséquences

Pour plusieurs auteurs, (Slovic et al. 1985 ; Sjöberg et al. 2004 ; Yates et Stone 1992), l**es conséquences** potentielles du risque n'apparaissent pas uniformément pour chaque individu accentuant la notion de subjectivité du risque. Nous comprenons alors qu'il y ait de

multiples débats sur la mise en œuvre de mesures correctives à un risque donné. Ainsi, pour Cadet et Kouabenan (2005 p. 10) « les débats et les polémiques que nous présentent les médias sont alimentés par des **différences d'appréciation** sur des activités que tous s'accordent à considérer comme risquées mais pour lesquelles il n'existe aucune estimation quantitative susceptible de constituer une référence commune ». Outre la nature des conséquences, « s'il est reconnu que les pertes dans une catégorie donnée peuvent arriver, il y a toujours l'incertitude que les pertes surviendront » (Yates et Stone 1992 p. 13). Supposons que l'emploi A de Jane Smith ait une probabilité de 15% de se situer dans la catégorie « localisation », dans une ville considérée comme « perte ». Si l'emploi B a une probabilité de 10% de se trouver dans la même ville, alors ce choix est alors considéré comme moins risqué.

L'absence d'atteinte du résultat prévu ou la privation de ce qui a été possédé traduit la notion de perte pour un individu (Yates et Stone 1992). Cette notion est directement rattachée à **l'heuristique de référence** dans laquelle la perte est relative à un niveau défini subjectivement (Kahneman et Tversky 1979 ; Yates et Stone 1992). Ainsi, si le résultat obtenu est supérieur à la référence, il s'agit alors d'un gain, à l'inverse, situé dessous de cette référence, il traduit une perte. Yates et Stone (1992) distinguent six catégories de références :

1. Moyenne personnelle : basée sur les habitudes de l'individu. Par exemple, pour Jane Smith, le niveau de satisfaction pour le choix de son futur emploi est défini par ses expériences passées.
2. Moyenne situationnelle : similaire à la moyenne personnelle mais définie avec des éléments extérieurs. Par exemple Jane Smith n'a aucune information sur la qualité des employés de sa future entreprise. Elle se réfère alors à des camarades qui ont œuvré dans cette entreprise et qui la renseigne sur ses collaborateurs.
3. Attente sociale : définie par des individus du cercle de référence. Pour Jane Smith, par exemple, le revenu salarié de référence issu de ses parents.
4. Cible : référence qu'un individu s'efforce d'atteindre.
5. Meilleure possible : définie socialement comme difficile à atteindre.
6. Regret : définie comme déjà atteint et qu'un individu écarte pour choisir une alternative.

En complément, Yates et Stone (1992) définissent une taxonomie de perte, basée sur le comportement des consommateurs et qui peut être étendue à d'autres activités :

- Perte financière : pertes causées lorsque le produit acquis ne fonctionnement plus du tout
- Perte de performance : pertes causées par un dysfonctionnement provoquant une baisse de ses performances
- Perte physique : le produit ne peut être utilisé car pouvant provoque des dommages physiques
- Perte psychologique : le produit ne correspond plus à l'image qu'en avait le consommateur vis-à-vis de lui-même
- Perte sociale : l'utilisation du produit affecte négativement le regard des autres sur le consommateur
- Perte de temps : l'utilisation du produit nécessite du temps pour l'adapter, le réparer ou le remplacer

Notons la similitude de certaine de ces pertes avec celles développées dans la littérature SSI et que nous rappelons ici (cf. 3.4.1 Première étape : le besoin de protéger le SI p. 193) : 1) pertes financières ou économiques directes ; 2) pertes financières indirectes ; 3) pertes d'image ; 4) pouvant entrainer des implications juridiques et 5) impacts stratégiques.

Après avoir présenté les concepts d'incertitude et de conséquences, permettant alors de disposer d'une vision avancée sur la décision pour le risque, nous pouvons aborder la notion de risque acceptable, ou mécanismes définissant l'aversion au risque.

Le risque acceptable

Selon Cadet et Kouabénan (2005), à l'appui des travaux de Fischhoff et al. (1981) la combinaison du bénéfice attendu et du risque perçu, permet de définir le risque acceptable. Plus généralement, Yates et Stone (1992) définissent trois catégories principales de comportement face au risque pour individualiser la notion de risque acceptable : 1) les comportements où la **préférence est le risque** relèvent d'une attirance pour un **résultat incertain**, comparé à un équivalent sûr de la valeur attendue de cette perspective 2) la **préférence pour un résultat certain** indique **l'aversion de risque** et 3) entre les deux, l'indifférence entre ces alternatives implique la neutralité de risque (Yates et Stone 1992).

Avant les travaux de Fischhoff et al. (1981), Starr (1969), constate que l'acceptabilité d'une situation à risque repose sur une perspective perçue du décideur des bénéfices ou des avantages attendus « à la puissance trois » (Kermisch 2011 p. 32). Le fondement de l'acceptabilité reposant jusqu'alors sur les seuls constats de Starr (1969), la suite de ses travaux fait émerger la nécessité de considérer les activités à **risque volontaires**, de celles qui sont **involontaires**. Cette caractéristique du risque a été par la suite éprouvée et démontrée, notamment par Slovic et al. (1984 ; 2000). Selon Starr (1969) « les activités volontaires recouvrent essentiellement les sports » et les activités involontaires, pour lesquelles le risque est subi, sont « liées à l'environnement de l'individu et à ses activités professionnelles » (Kermisch 2011 p. 31). Pour exemple, Sjöberg et al. (2004 p. 9) comparent deux individus engagés dans deux activités différentes, « un passager de train et un grimpeur de montagne » pour lesquels il y a des « distinctions évidentes qui concerneraient des concepts **comme le contrôle** » et l'aspect volontaire de l'activité. Ils concluent que les résultats convergents de la recherche montrent que les humains **tolèrent considérablement plus de risque quand ils s'engagent dans un comportement volontaire** (Sjöberg et al. 2004 p. 9).

Selon Slovic et Peters (2006), il y avait un consensus dans la recherche académique sur la **relation entre risque et avantage**, notamment depuis les travaux de Slovic et al. (1982). En effet, les études de Slovic et al. (1979 et 1982) précisent que le risque perçu est en relation inverse avec les bénéfices attendus. Cette relation est positive pour les activités à haut risque, signifiant que plus une activité réalisée est perçue risquée, plus les avantages perçus sont élevés et réciproquement (Cadet et Kouabenan 2005 ; Slovic et Peters 2006). Les découvertes d'Alhakami et Slovic (1994) démontrent la relation inverse indiquant que plus les activités sont risquées, moins les individus jugent leurs avantages élevés. Slovic et Peters (2006 p. 323) précisent que les individus observent un risque selon des bénéfices attendus, tels que vu précédemment, et également en **jugeant l'activité risquée** comme « **bonne ou mauvaise** ». C'est ainsi que **l'heuristique d'affect** s'établit pour le jugement d'un risque. Si les individus ont un sentiment favorable pour une activité, ils jugent faible le risque et élevés les avantages. L'affect guide donc l'acceptabilité du risque, dont une illustration est donnée par Finucane et al. (2000, cf. figure 11). L'heuristique d'affect présenté par Finucane et al. (2000) précise son interaction entre risque et bénéfice, pour évaluer l'acceptation de l'énergie nucléaire selon l'affect d'une part et le bénéfice ou le risque sont annoncés comme faibles ou élevés d'autre part :

- Lorsque l'affect est **positif** :

- si le bénéfice est annoncé comme élevé, le risque perçu est faible.
- si le risque est annoncé comme faible, le bénéfice perçu est élevé

– Lorsque l'affect est **négatif** :
  - si le bénéfice est annoncé comme faible, le risque perçu est élevé
  - si le risque est annoncé comme élevé, le bénéfice perçu est faible

Cet exemple démontre deux avancées majeures dans les travaux sur la perception des risques. La première **situe l'affect comme central** dans l'acceptation des risques, en complément des bénéfices « attendus », qu'ils soient perçus ou annoncés, et du niveau de risque perçu (Slovic et Peters 2006). L'affect permet **une perspective différente** sur le **jugement du risque**. Si l'affect est favorable à une activité, le jugement du risque sera diminué et le bénéfice augmenté. À l'inverse, un affect défavorable provoquera un jugement opposé, un risque perçu augmenté et un bénéfice perçu diminué. La seconde fait émerger l'importance de l'information disponible, ou fournie, pour le bénéfice ou risque « annoncé ». En ce sens, Short (1984) avait précédemment mis en évidence que les risques sont perçus selon les informations le caractérisant. Les risques sont alors jugés en regard des différentes sources, caractérisées par Short comme des « fabriques de risque » sur lesquelles les individus forment les représentations sociales du risque, en considérant peu les caractéristiques techniques du risque (Short 1984). Particulièrement pour l'affect, les risques perçus peuvent être influencés par la valeur du bénéfice annoncé, et le bénéfice perçu ou attendu peut être influencé par la **valeur du risque annoncé**. Une seconde expérience de Finucane et al. (2000) montre l'effet augmenté de l'affect lorsque les individus doivent évaluer un risque rapidement, dans un temps réduit ne laissant pas de place à une « réflexion analytique » (Slovic et Peters 2006 p. 323). Ainsi, ces expériences indiquent que l'affect influence le jugement directement et n'est pas simplement une réponse à une évaluation analytique antérieure, en accord avec les découvertes d'Alhakami et Slovic (1994).

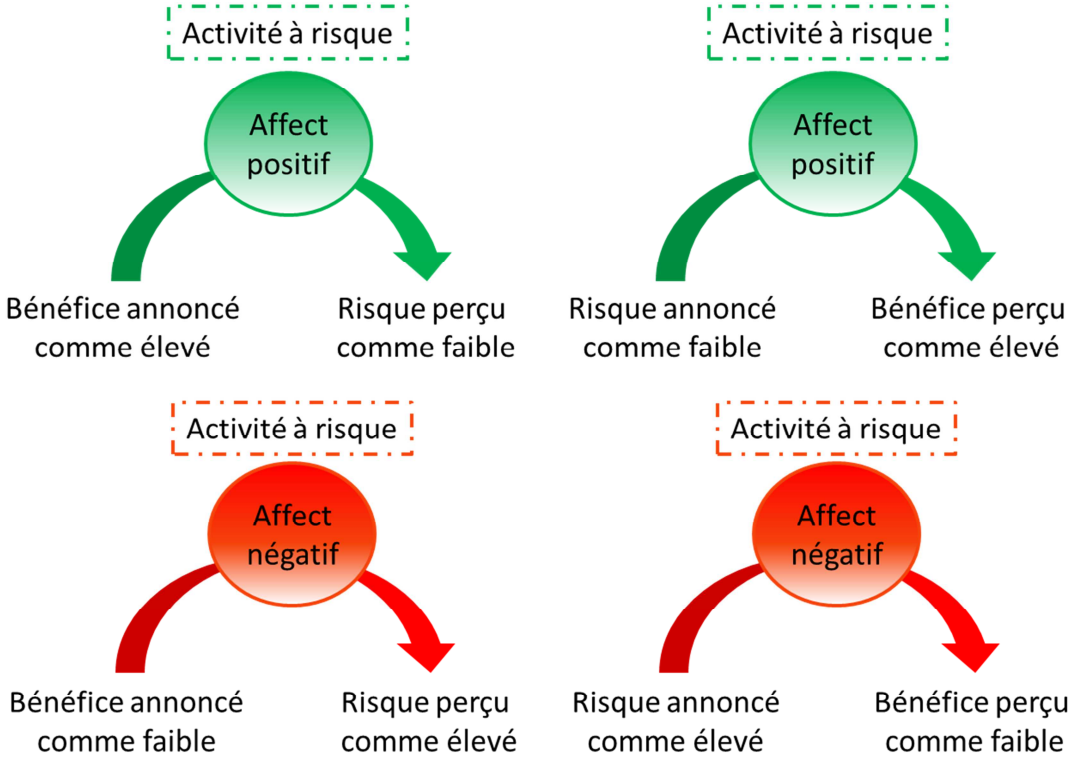


Figure 11 : Influence de l'affect sur l'évaluation risque / bénéfices

(adapté de Finucane et al. 2000 p. 9)

Finucane et al. (2000) ont testé l'affect pour une variété de technologies, permettant de confirmer la pertinence de de cette heuristique. Une autre application de l'affect, auprès d'experts en toxicologie supporte le fondement de cette heuristique. En effet, les résultats de l'heuristique **d''affect sur les experts** en toxicologie sont **semblables à ceux des profanes**. Précisément, les réactions d'affect des toxicologues pour les produits dangereux ont modifié leur jugement. Ces mêmes experts ont été interrogés en deux temps pour qu'ils :

1. se prononcent sur « une évaluation intuitive rapide » sur trente produits chimiques tels que le benzène, la fumée de cigarette ou encore les dioxines dans la nourriture sur une échelle d'affect (favorable ou défavorable).
2. jugent le risque associé à une exposition au produit chimique équivalent à moins du centième des recommandations des agences sanitaires.

En regard d'un si faible niveau d'exposition, ces jugements de risque étaient attendus « uniformes et bas », et dissociés des évaluations d'affect, mais à l'inverse, la corrélation affect/ risque a été constatée (Slovic et al. 2004 p. 316).

Nous conclurons la synthèse de l'heuristique d'affect par la remarque de « Slovic et Peters 2006 p. 323) : « Comme un élément clé de la pensée résultant de l'expérience, l'affect heuristique était essentiel pour l'évaluation du risque et la survie pendant l'évolution de l'espèce humaine », mais « l'affect peut aussi induire en erreur les individus ».

Le risque a été présenté sur ses trois concepts principaux que sont l'incertitude, les conséquences et le choix à adopter face au risque (afin qu'il soit acceptable). Dès lors, nous pouvons aborder les mécanismes permettant de les articuler, en regard des trois paradigmes d'évaluation du risque : l'utilité espérée, cognitif, et psychométrique.

La littérature dans le champ de la gestion des risques énonce principalement trois approches pour l'évaluation : l'utilité espérée, le paradigme cognitif et le paradigme psychométrique. Ces trois paradigmes, bien que différents dans leur méthode et critères, visent à évaluer le risque en traitant des informations diverses pour « l'obtention d'une valeur unique globale, caractéristique de la situation traitée » (Cadet et Kouabénan 2005 p. 8).

3.2.3. L'utilité espérée

Le paradigme d'utilité espérée prend ses racines dans les premières modélisations du risque, dans le domaine économique et financier. Ce modèle d'évaluation du risque fait interagir la notion d'utilité de l'évènement et l'utilité de ses conséquences avec un objectif de maximisation économique ou financier pour le décideur, soit la « satisfaction procurée par un gain » (Kermisch 2011 p. 11). Ainsi, selon Cadet et Kouabénan (2005), il vise à évaluer l'investissement financier en regard des conséquences positives ou négatives qu'il faut anticiper, afin d'objectiver la décision en articulant la possibilité que :

1. des évènements non souhaitables se produisent,
2. leurs conséquences soient importantes.

Ainsi, bien qu'utilisé jusqu'à aujourd'hui, notamment dans l'évaluation des risques industriels (Cadet et Kouabénan 2005 ; Sjöberg et al. 2004), cette conception présente deux faiblesses majeures[37].

[37] Notons que le paradigme de l'utilité espérée a été notamment critiqué par Allais en 1953, puis Simon en 1955, Ellsberg en 1961, et Kahneman et Tversky dans les années 1970. Notre propos ne vise

D'une part, l'évaluateur est absent du modèle alors qu'il en est une composante essentielle, dans la mesure où il lui appartient de l'adapter aux conditions de l'application à sa situation. En effet, si la connaissance des probabilités (Cadet et Kouabénan 2005) est un axiome de l'utilitée espérée, seul le décideur peut **apprécier les conséquences** positives ou négatives, selon des options qui s'offrent à lui dans une situation particulière (Kermisch 2011). Pour Hermand et Chauvin (2008 p. 349), ce paradigme ne permet alors pas de prendre en compte « la loi psychologique fondamentale de l'aversion pour le risque ». Nous pouvons éclairer ce commentaire, sur la faible considération du décideur dans ce modèle, par les apports de Tversky et Kahneman (1979) et la théorie des « perspectives ». En effet, sur la base du paradoxe d'Allais, qui a mis en évidence la décision non rationnelle de l'évaluateur[38], Tversky et Kahneman ont enrichi l'utilité espérée de deux phases, l'une visant à « intégrer et reformuler les données qu'ils perçoivent » et l'autre visant à « quantifier et la satisfaction des biens et des pertes » (Kermisch 2010 p 19). Précisément, ces auteurs ont mis en évidence la rationalité limitée de Simon pour les évaluateurs « les conduisant à raisonner en regard d'heuristiques pour réduire les tâches complexes d'estimation de probabilités et de prédictions de valeurs à des opérations de jugement plus simples » (Kermisch 2010 p. 18)

D'autre part, l'utilité espérée ne permet pas de **quantifier** et comparer de façon uniforme **des conséquences** hétérogènes et variées dans des champs différents, fussent-ils de la même branche (Hermand et Chauvin 2008). Pour exemple, quelle référence commune pour les risques énergétiques peut être établie pour les conséquences des « productions nucléaires, hydrauliques, éoliennes ou marémotrices ? » (Cadet et Kouabénan 2005 p. 12). Rappelons que cette référence commune est nécessaire pour le processus d'analyse de risque mais aussi pour la mise en œuvre de solution de gestion du risque. En ce sens, si les comparaisons entre ces activités n'est pas réalisable, alors c'est la démarche d'évaluation qui en serait défaillante (Cadet et Kouabénan 2005).

Pour dépasser cette double problématique d'appréciation et de quantification des conséquences, les économistes ont proposé d'introduire un critère de décision et un critère d'utilité. Ainsi, le critère de décision, basé sur l'aversion au risque de l'individu, indique que le choix retenu est le plus « certain » et le critère d'utilité traite de la conséquence la plus

pas à retracer fidèlement l'historique de ce paradigme mais à décrire les concepts permettant d'appréhender la perception des risques.

[38] Le paradoxe d'Allais démontre les contradictions de la théorie de l'utilité espérée pour l'espérance mathématique. L'exemple suivant illustre la préférence de choix pour la certitude, supposons deux possibilités : A –gagner 100 € avec 100% de chance et B – gagner 150 € avec 90% de chance, et 0 € avec 10% de chance. Alors que l'espérance de B est supérieure à A, la préférence des évaluateurs est majoritairement A.

« utile » (Hermand et Chauvin 2008 p. 349). Combinées entre eux, les deux critères permettent l'évaluation de la maximisation, dont le décideur retiendra la plus importante. Ainsi, la mesure du risque repose sur la probabilité et une échelle d'évaluation des conséquences, permettant de quantifier la gravité des effets et de déterminer si un risque peut être considéré comme acceptable.

Si les valeurs attribuées à l'utilité se définissent comme subjectives, au sens de « propre à un individu » il convient alors d'observer la validation de ces valeurs par l'évaluateur. Selon Cadet et Kouabénan (2005 p. 13), il existe deux formes de validation dont la première, dite « formelle », a longtemps prévalu alors qu'elle fait appel à des systèmes de règles complexes, engageant les évaluateurs à préférer la validation dite « empirique ». Cette validation est nommé « empirique » car elle s'appuie sur les expériences antérieures et les connaissances de l'évaluateur. Cadet et Kouabénan (2005 p. 13), notent que les évaluateurs, doivent définir la valeur de maximisation d'une situation tout en ne disposant que de connaissances limitées (cf. Slovic et al. 1979) et avec une faible capacité d'activation de ces connaissances (cf. Tversky et Kahneman 1973). Rapprochant ainsi « l'expertise décisionnelle » de la gestion du risque, Cadet et Kouabénan (2005 p. 13) soulignent alors qu'un « bon évaluateur du risque » ne serait que le « **bon décideur spécialisé dans une situation spécifiée** ». Notons que cette notion, visant à comparer connaissance et décision est proche de celle des schémas d'Amalberti (1996 p. 86), que nous développons dans la section traitant du paradigme cognitif, et qui sont « des structures de données destinées à représenter des situations extérieures, des séquences d'évènements, des procédures » qui représentent « les stéréotypes de ces situations ». Cadet et Kouabénan (2005 p. 14) étayent leurs propos sur « l'expertise décisionnelle du risque » en citant des activités dont l'évaluation des risques repose sur les connaissances, telle que pour la chirurgie, permettant, justement, de décider « le moment de l'acte chirurgical et l'importance de ses différentes conséquences ». Cette évaluation vise à minimiser le risque, en observant l'utilité espérée de l'acte, sauver la vie d'un patient, et les probabilités de réussite, basées sur les observations antérieures. Précisément, il s'agit de quantifier le risque « à partir de l'appréciation de l'utilité des conséquences de chaque mode d'action possible dans une telle situation » (Cadet et Kouabenan 2005 p. 14).

La prise en compte de deux dimensions comme composantes de l'évaluation amène à définir le risque acceptable comme une référence à une valeur intermédiaire entre avantages et conséquences négatives, notamment dans les situations où l'activité est génératrice de biens et de nuisances (Fischoff et al. 1981). En ce sens, la perception et l'acceptabilité du risque

diffèrent selon plusieurs facteurs, tels que par exemple les connaissances scientifiques, la législation, les expériences, la responsabilité vis-à-vis du risque, la profession exercée (Cadet et Kouabénan 2005).

Les apports et limites du paradigme d'utilité espérée font consensus dans la littérature (Cadet et Kouabénan 2005 ; Chauvin et Hermand 2006 ; Kermisch 2010). En termes d'apports, il permet de comparer les risques et de définir les niveaux de risque acceptable grâce à la détermination d'une valeur intermédiaire entre avantages et inconvénients (Fischhoff et al. 1981). En termes de limites, d'une part, ce paradigme est construit sur un axiome du fonctionnement rationnel[39] de l'évaluateur pour une situation à risque (Cadet et Kouabénan 2005). En effet, Kermisch (2011 p. 15) rappelle que ce modèle « suggère qu'une option est évaluée non plus par rapport à ses conséquences mais en fonction de l'utilité de ses conséquences » évaluation basée sur le « comportement rationnel » du décideur. Cet axiome est mis en perspective d'une évaluation reposant sur la combinaison de règles complexes (Cadet et Kouabénan 2005), pour une multitude et une variété de conséquences dont il n'est pas certain que l'évaluateur **puisse accéder et en définir l'ampleur** (Slovic et al. 1979 ; Yates et Stones 1992). Pour cette raison l'utilité espérée ne peut décrire le comportement de l'évaluateur en situation risquée ou incertaine (Kermisch 2010).

En ce sens, Cadet et Kouabénan (2005) soulignent la fluctuation des valeurs subjectives, telles que définies dans l'utilité espérée, qui par construction, écarte la notion d'une référence commune propre à toutes les évaluations. À cet effet ils illustrent leur propos sur l'importance accordée aux **informations disponibles** en retraçant l'« 'histoire américaine sur la saccharine » et que nous synthétisons chronologiquement (Cadet et Kouabénan 2005 p. 16) :

- la saccharine est un produit fortement utilisé aux États-Unis car faiblement calorique et gustatif,
- elle est recommandée notamment aux diabétiques et dans les régimes hypocaloriques,
- en 1970 une étude sur les rats montre que la saccharine accroit le taux de cancer et les autorités classent alors la saccharine sur la liste des cancérigènes,

[39] Soit les axiomes de complétude, de transitivité, de continuité et d'indépendance, démontrée dans les travaux de Ramsey en 1931 et de Von Neumann en 1947) :

- transitivité : si un individu préfère l'alternative x à l'alternative y, et l'alternative y à z, alors il doit rationnellement préférer x à z
- continuité : permet de représenter l'ordre des préférences par une fonction d'utilité.
- indépendance : permet de représenter les préférences de l'individu par une fonction d'utilité

- la saccharine est ainsi interdite dans les aliments, conformément à la réglementation sur les additifs alimentaires susceptible d'augmenter les risques de cancer, quelle que soit la quantité,
- les protestations des consommateurs et des industriels, très attachés aux boissons allégées, sont prises en compte par le congrès qui vote une interdiction d'interdire la saccharine,
- plusieurs études réalisées ultérieurement montrent que le taux de cancer lié à la consommation de saccharine est accru sur les seuls rats et spécialement les mâles.

Cette illustration, confirme la **dépendance de la décision aux informations disponibles** (Short 1984 ; Slovic et Peters 2006). Pour Cadet et Kouabénan (2005), elle démontre la dépendance de la décision à l'importance subjective accordée aux informations disponibles. Ainsi, selon ces mêmes auteurs, l'illustration confirme qu'un risque ne peut être observé **indépendamment de son évaluateur**.

En synthèse, le paradigme de l'utilité espérée permet d'établir des règles de décision simples, que la présence d'incertitudes ne rend pas caduques, dont les faiblesses ont été traitées dans la discipline psychologique (cf. Edwards 1961). Selon Cadet et Kouabénan (2005), ce paradigme apparait mobilisé dans l'évaluation des risques industriels et particulièrement pour les conséquences liées au fonctionnement de processus de fabrication, pour concilier des impératifs de production et de sûreté. S'agissant de l'étude des comportements des individus et de leur évaluation des risques, la recherche dans le domaine de la théorie de la décision a mis en évidence que **les règles de l'utilité espérée ne sont pas toujours respectées**. Notamment, les « biais cognitifs » mis en évidence par les travaux de Kahneman et Tversky sur les apports au paradigme de l'utilité espérée trouvent leur application dans le paradigme psychométrique, dont la paternité revient à Slovic, Lichtenstein et Fischhoff dans les années 1980. Kermisch (2011) conclu que, pour cette raison, **l'étude de la perception des risques ne peut se soustraire à une approche plus holistique considérant l'évaluateur et les déterminants sociaux et culturels qui lui sont propres** (Douglas et Wildavsky 1983 ; Cadet et Kouabénan 2005). Ces constats renforcent alors davantage le recours au paradigme psychométrique qui permet d'appréhender les « options complexes et subtiles d'individus profanes sur les risques (Hermand et Chauvin 2008 p. 354), risques justement définis comme subjectifs (Slovic et al. 1987).

3.2.4. Le paradigme cognitif

Selon Hermand et Chauvin (2008 p. 350), ce paradigme prend son fondement dans le « déclin progressif du behaviorisme et la modélisation des comportements humains selon la relation stimulus et réponse », engageant alors à observer les « processus psychologiques sous-jacents ». Ainsi, les modèles de prises de décision introduisent progressivement[40] non seulement le risque mais aussi les attitudes, voire l'affect d'attirance ou d'aversion pour l'activité « risquée » (Cadet et Kouabénan 2005). Ce commentaire s'inscrit dans le reproche d'Herbert Simon, à l'endroit du paradigme de l'utilité espéré, qui soulève la question des alternatives aux processus décisionnels. Pour Simon (1955) ces alternatives ne sont pas « données mais pensées » (Kermisch 2010 p. 16), alors que l'utilité espérée ne permet pas la description de ces processus de pensée. Simon (1955), **à l'appui de théorie de la décision descriptive et de la rationalité limitée, fait émerger le concept des limites cognitives du preneur de décision,** lui imposant de construire un modèle simplifié du monde. Enfin, Daniel Kahneman et Amos Tversky étendent les principes de limitation cognitive d'Herbert Simon pour les risques économiques aux situations où les dommages potentiels sont représentés (Kermisch 2010).

Ainsi, l'approche du paradigme cognitif est sensiblement différente des deux autres car il vise non pas un consensus sur le risque acceptable mais traite des mécanismes qui y conduisent. Il s'agit alors d'étudier les modalités d'élaboration du processus d'évaluation dès sa formation (Cadet et Kouabénan 2005). Pour illustrer synthétiquement l'emploi de se paradigme, nous pouvons citer les travaux d'Amalberti (1996) et particulièrement l'exemple du pilotage d'avion lors de la phase critique d'atterrissage, pour laquelle les seules options possibles sont « poursuivre l'atterrissage » ou « remettre les gaz ». Les pilotes, en regard de la nécessité d'une réaction rapide et en situation, doivent davantage décider de l'action que d'effectuer une évaluation des avantages et inconvénients de chaque option, au « risque » d'un crash.

L'évaluation cognitive du risque repose sur un modèle dans lequel les activités cognitives d'acquisition et de traitement de l'information conduisent à une valeur unique permettant la décision. Pour plusieurs auteurs (Hermand et Chauvin 2008 ; Cadet et Kouabénan 2005), le modèle conceptuel du jugement d'Hogarth (1980) est le plus adapté en matière d'étude de risque. Cadet et Kouabénan (2005) justifient la pertinence de ce modèle par deux raisons principales.

[40] Notamment grâce aux travaux d'Edwards en 1961

D'une part, la relation « libre »[41] du système entre environnement (cf. cadre 1, figure 12) et résultat (cf. cadre 7, figure 12) permet justement de considérer **la subjectivité** des informations traitées dans l'évaluation (au sens de « propre à un sujet ») et **la variété** donnant lieu à des résultats possiblement changeants et donc un diagnostic possiblement différent. En ce sens, il convient de qualifier l'activité diagnostique comme le résultat de la meilleure adéquation entre recueil d'information, schéma et valeur donnée au schéma (Amalberti 1996 ; Cadet et Kouabénan 2005 ; Hermand et Chauvin 2008 ; Hogarth 1980).

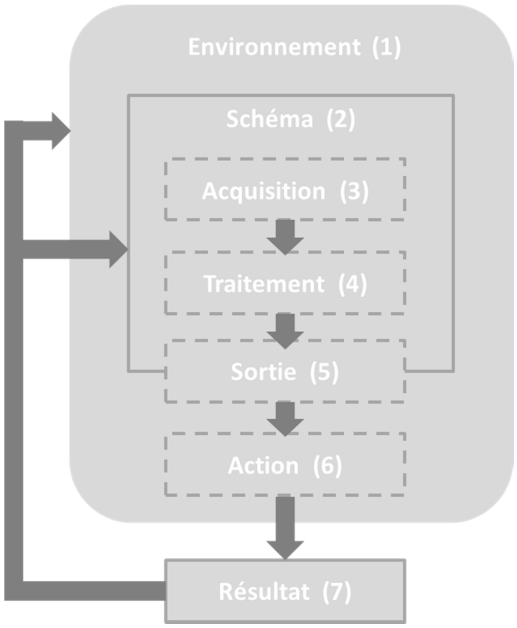


Figure 12 : Modèle conceptuel du jugement
Hogarth (1980)

D'autre part, l'évaluation est réalisée **selon des heuristiques**, permettant d'éviter une démarche stochastique, fortement consommatrice de ressources cognitives pour des évaluateurs dont les capacités sont limitées (Amalberti 1996 ; Hermand et Chauvin 2008 ; Cadet et Kouabénan 2005). Spécifiquement à la conduite de système à risque, ce principe d'évaluation est repris selon le concept de schéma d'Amalberti (1996) offrant alors deux avantages. Le premier est un cout cognitif limité grâce à la reconnaissance précoce d'une situation, basée sur ses connaissances, croyances, expériences et de l'environnement. Il s'agit « d'une phase initiale de reconnaissance avec introduction d'une dimension

[41] Cadet et Kouabénan (2005 p. 23) évoquent des « degrés de liberté » dans le modèle

sémantique » permettant de « cadrer » les activités d'évaluation en focalisant les processus ultérieurs de recherche sur quelques éléments spécifiques » (Cadet et Kouabénan 2005 p. 25). Le second est le cadrage des processus d'acquisition et de traitement de l'information qui sont « guidés vers la recherche d'éléments diagnostiques » (Hermand et Chauvin 2008 p. 351). En effet, selon Cadet et Kouabénan (2005 p. 25), l'évaluateur « ne s'attache qu'au recueil et au traitement d'informations de qualité, c'est-à-dire connues pour leur valeur "diagnostique" et leur pouvoir prédictif ».

Les limites du paradigme cognitif identifiées dans la littérature sont directement liées aux schémas et aux ressources cognitives.

La première limite s'inscrit directement dans le fonctionnement cognitif que les travaux princeps de Tversky et Kahneman (1974) ou de Kahneman et Slovic (1982) ont pu mettre en évidence, à l'instar de ceux pour le paradigme de l'utilité espérée. Pour ces auteurs les heuristiques sont des mécanismes permettant aux individus de simplifier une tâche et définies comme « des stratégies mentales commodes de traitement des informations » (Hermand et Chauvin 2008 p. 352). La littérature fait consensus sur trois heuristiques que sont 1) la **représentativité**, 2) la **disponibilité**, et 3) l'**ancrage-ajustement**.

L'heuristique de **représentativité** consiste à rattacher la situation à évaluer à une classe ou schéma selon la définition d'Amalberti (1996), déjà connue de situations antérieures qui paraissent similaires. Cette heuristique implique l'utilisation même des schémas, pour lesquels l'individu doit reconnaitre le « modèle » en regard des indices dont il dispose. Ainsi, une erreur de reconnaissance « est difficilement repérée et récusée par l'individu » (Hermand et Chauvin 2008 p. 352). Cette erreur peut conduire l'évaluateur à traiter une situation cognitive A qu'il pense reconnaitre, alors qu'il s'agit une situation cognitive B, et ainsi aboutir à un résultat inadapté. Ceci est en accord avec le commentaire de Slovic et al. (1982a p. 85) qui précise que « les erreurs des individus peuvent souvent être rapprochées d'informations inadéquates et d'expériences biaisées ». Amalberti (1996) précise plusieurs exemples d'individu en condition de « conduite de système à risque », tels que des pilotes d'avion compromis dans des schémas conduisant à l'incident voire l'accident aéronautique.

La **disponibilité**, ou facilité avec laquelle l'information est rendue accessible, consiste à évaluer la situation à risque à partir des informations les plus couramment répandues ou les plus récentes qui sont de facto les plus disponibles car facilement rappelées (Kahneman et Slovic 1982). Selon Cadet et Kouabenan (2005 p. 22) c'est une des données importantes

pour la compréhension de l'évaluation car les risques qui font « l'objet d'une large médiatisation sont perçus comme plus importants que ceux qui, tout en étant aussi dangereux, sont moins présents dans les médias ».

L'**ancrage-ajustement** consiste à évaluer en prenant comme référence le cas précédent (ancrage) en y apportant des adaptations (ajustement) pour tenir compte de la situation actuelle. Si l'ancrage est souvent soumis aux effets de contexte, autrement nommé « framing effect » par Tversky et Kahneman (1981), l'ajustement est souvent influencé par l'heuristique d'affect, introduisant un biais dans l'évaluation (Finucane et al. 2000), tel que développé ci-après.

Nous traitons les biais de jugement de ces trois heuristiques de façon plus approfondie dans les sections « représentativité », « disponibilité », et « effet de cadrage » de la section « Les biais d'évaluation des risques » (p. 157).

La seconde limite prend ses racines dans la subjectivité des valeurs mobilisée. Cadet et Kouabénan (2005 p. 27) citent le « nombre psychophysique » sur lequel repose l'évaluation. La subjectivité des valeurs rend l'estimation non linéaire dès lors que la valeur éprouvée dépend d'autres caractéristiques de la situation, noté « stimuli externes » et conduisant à l' « insensibilité d'un nombre important de morts » pour une catastrophe de grande ampleur ou pour des risques répétitif tel le risque routier (Cadet et Kouabénan 2005 p. 27). Une autre application de ce principe est illustrée par l'unité objective, considérée lors de chaque évaluation. Cadet et Kouabénan (2005) précisent qu'au-delà de cette valeur, le niveau de risque perçu n'est pas linéaire. Par exemple, si le niveau de risque pour le cancer du fumeur est situé à quinze cigarettes par jour, « les cigarettes additionnelles sont évaluées comme de moins en moins nocive à mesure que croît la consommation journalière » (Cadet et Kouabénan 2005 p. 28).

Plus récemment, Finucane et al. (2000) ont introduit un heuristique d'affect, soulignant ainsi une nouvelle fois l'importance de caractéristiques affectives particulièrement opérantes dans l'évaluation de situations fortement recherchées ou fortement redoutées (cf. « 3.2.2 Concepts de l'étude des risques » p. 111).

3.2.5. Paradigme psychométrique

Le paradigme psychométrique prend ses racines dans le champ de recherche associé au paradigme de l'utilité espérée et de l'utilité subjectivement espérée (Slovic, Lichtenstein et

Edwards 1965). Slovic, Fischhoff et Lichtenstein ont été sollicités pour étudier, au début des années 1970, des comportements face au risque jugés étonnants, constatés non pas pour des risques financiers simples tels que des paris observés en laboratoire en mobilisant l'utilité espérée, mais hors laboratoire et pour des risques naturels (Slovic 2000 ; 2006). Cette perspective modifie alors substantiellement la définition du risque utilisée jusqu'alors, pour intégrer la notion de **conséquences humaines**, voir **l'évaluateur lui-même** (Sjöberg et al. 2004). Cette évolution de la notion de risque s'inscrit dans la continuité des travaux de Starr (1969) qui a fait émerger un intérêt, devenu ensuite croissant, pour la gestion des risques et particulièrement la façon dont les gens les perçoivent, tolèrent et les acceptent (Sjöberg et al. 2004). En effet, la **divergence entre experts et profanes**, les premiers assurant qu'il n'y avait aucun risque pour des situations où les deuxièmes en percevaient, a positionné la perception des risques comme une contrainte **à une prise de décision raisonnable** (Cadet et Kouabénan 2005 ; Sjöberg et al. 2004). Ensuite, les dilemmes sociaux de gestion des risques s'appuient sur cette même divergence entre décision du publique et décision des experts. Slovic et ses confrères étudient ainsi les risques naturels à la lumière des travaux sur les heuristiques (représentativité, disponibilité et ancrage-ajustement abordés ci-avant) et les biais définis par Tversky et Kahneman (1974). C'est ainsi que la recherche sur les risques s'est enrichie d'une nouvelle approche, le paradigme psychométrique, dont l'objectif initial était l'étude des risques perçus par les citoyens pour les pesticides et l'énergie nucléaire, soit les « opinions complexes et subtiles des individus sur les risques », définies comme « la caractérisation de la perception des risques » (Hermand et Chauvin 2008 p. 345).

Pour Sjöberg et al. (2004 p. 10) le paradigme psychométrique est un cadre théorique dans lequel le risque est défini **subjectivement par des évaluateurs, influencés « par une vaste gamme de facteurs psychologiques, sociaux, institutionnels et culturels »,** permettant d'identifier et de quantifier ces facteurs pour les comparer entre groupes d'évaluateurs (Slovic et al. 1980 ; 1987). Ainsi, le modèle du paradigme psychométrique combine des évaluations subjectives et des techniques d'analyse « **permettant des représentations quantifiées ou cartes cognitives des attitudes et perceptions du risque** » (Cadet et Kouabénan 2005 p. 20).

Afin de décrire précisément le fonctionnement du paradigme psychométrique, il convient d'en aborder les déterminants sociaux, les caractéristiques sociales et les mécanismes d'évaluation, objet des sections suivantes. Avant de conclure, nous ne pouvons présenter le paradigme psychométrique en faisant l'impasse sur la théorie culturelle du risque (Douglas

1978 ; Douglas and Wildavsky 1982). En effet, la théorie culturelle du risque permet d'éclairer la perception et de la gestion des risques en tenant en compte des incertitudes, selon les styles de pensée qui régissent l'action sociale des individus (Douglas et Wildavsky 1983).

Dimension sociale des risques

Le paradigme psychométrique s'est établi par la volonté de comparer des risques sociétaux (énergie et environnement) selon la vision des experts et des profanes, et ensuite selon la vision d'individus de différentes nations (Hermand et Chauvin 2008). Ainsi, l'hypothèse fondamentale du paradigme psychométrique est que la chose perçue comme risquée, selon l'évaluateur, **dépend de plusieurs facteurs psychologiques et sociaux** (Slovic 2000) **et aussi culturels, politiques et institutionnels** (Hermand et Chauvin 2008 ; Sjöberg et al. 2004). Précisément, l'acceptation du risque ne se définit pas par les seuls dommages possibles liés à l'utilisation d'une technologie ou à des phénomènes naturels, mais par une représentation de ce risque construite sur des choix sociaux. Pour étayer ce propos, Cadet et Kouabénan (2005) évoquent l'acceptation d'un risque en tenant compte dans **le même temps du niveau d'évolution technologique, des valeurs auxquelles elle se réfère et des mesures préventives mises en œuvre** pour couvrir ce risque. Par exemple, particulièrement à l'évaluation des pertes potentielles liée à un risque, Yates et Stone (1992) proposent une taxonomie des conséquences qui peuvent être combinées entre elles et appréciées subjectivement par l'évaluateur, en fonction de ses enjeux pour l'activité risquée (cf. 3.2.2 Concepts de l'étude des risques p. 111, section « les conséquences »).

Pour Cadet et Kouabénan (2005), les déterminants sociaux peuvent s'étudier selon deux niveaux, définis comme « risque sociétal » et comme le risque pour un groupe donné d'individus, le « groupe émergent ». Ainsi, le risque sociétal s'attachera à observer l'évaluation d'individus réunis en groupe fonctionnel pour une prise de décision inhérente, par exemple, à la pollution, à l'énergie nucléaire ou encore aux transports routiers ou ferroviaires (Cadet et Kouabénan 2005). Le groupe « émergent », selon la définition de Cadet et Kouabénan (2005), constitue un nombre plus restreint d'individus dont l'activité risquée est semblable, des individus réunis par leur profession tels que les pompiers ou les médecins, ou des individus ayant des caractéristiques communes pour le risque tels les fumeurs ou les jeunes conducteurs par exemple (Cadet et Kouabénan 2005). Ce double

niveau d'étude, non exclusif l'un de l'autre, souligne davantage l'approche comparée du paradigme psychométrique et le relie avec deux caractéristiques principales.

La première caractéristique, identifiée sur la base des travaux de Short (1984), **relève de la médiatisation de l'information recueillie**. Selon Short (1984), l'information provient soit d'une source de référence, telle que des amis, des organismes officiels ou encore des médias (Cadet et Kouabénan 2005 ; Hermand et Chauvin 2008). En effet, la perception des risques est médiatisée par les modes de recueil d'information, mettant l'accent sur les représentations sociales induites du risque et sur sa « matérialité » (Cadet et Kouabénan 2005 p. 17).

La seconde caractéristique qui relève de l'**appartenance au groupe** est mise en évidence par Douglas et Wildavsky (1982). Selon ces auteurs, les évaluations partagées de probabilités et de valeurs, dans certains contextes sociaux et culturels, forment les perceptions et les évaluations de risques (Douglas et Wildavsky 1983). Ils nomment ces influences « les biais culturels » et évoquent des « valeurs communes » qui « entraînent des peurs communes (et par conséquence un accord autour de ce qui ne fait pas peur) » (Douglas et Wildavsky 1983 p. 8). Dans ce cas, Rippl (2002) définit cette construction du risque par une vision filtrée du monde selon des croyances, valeurs et attitudes. Le paradigme psychométrique permet de classer les risques selon des caractéristiques « propres à chaque groupe social, aux valeurs et aux profits valorisés ou espérés, mais aussi aux peurs, aux craintes, aux préoccupations qu'il nourrit et aux accidents ou incidents ayant affectés la vie de ce groupe » (Cadet et Kouabénan 2005 p. 21).

Particulièrement à l'objet de nos travaux, dont le niveau d'étude est l'individu dans son organisation, les déterminants pourront être définis par des caractéristiques propres au secteur d'activité et aux groupes d'appartenance de l'individu. En effet, nous notons que de nombreux travaux préconisent l'analyse des risques portant sur les systèmes d'information en situant justement le **contexte** dans lequel sont réalisées les activités de l'organisation (Albrechtsen et Hovden 2009 ; Backhouse et Dhillon 1996 ; Choobineh et Dhillon 2007 ; Dhillon et Backhouse 2001 ; McFadzean et al. 2007).

Nous avons précisé comment la matérialité du risque peut être dépassée par une construction basée prioritairement sur les déterminants sociaux, il convient dès lors d'aborder la façon dont cette construction sociale est réalisée.

Construction sociale du risque

Les bases du paradigme psychométrique reposent sur la nécessité de distinguer le risque réalisé et le risque perçu (Cadet et Kouabénan 2005 ; Slovic et al. 1987 ; Slovic et al. 1982), mettant en perspective la possible divergence d'évaluation entre expert et profane. En effet, si Slovic (1992 p. 5) rappelle que la supposition première du paradigme psychométrique est « que le risque est intrinsèquement subjectif » et qu'il « n'existe pas "ailleurs", indépendamment de nos esprits et cultures, dans l'attente d'être mesuré ». Ainsi, les évaluateurs doivent « **s'appuyer sur des inférences fondées sur ce dont ils se souviennent, ce qu'ils ont entendu ou observé à propos du risque en question** » (Slovic et al.1979 p. 15), à l'appui de sources d'informations personnelles et des « particularismes de la situation » (Cadet Kouabénan 2005 p. 17). Sjöberg et al. (2004 p. 8) prolongent ce constat en indiquant que le risque « est une construction sociale et culturelle reflétant des valeurs, des symboles, l'histoire et l'idéologie », découlant de « la spécificité et de la variabilité d'existence sociale humaine desquelles on ne devrait pas simplement présumer que les résultats et des évaluations sur des instruments identiques ont les mêmes significations dans des contextes différents ».

Dès lors, le risque est une valeur construite sur la base de connaissances techniques et surtout de « représentations sociales, des systèmes de valeurs et de croyances » comme précisé ci-avant mais aussi de « la **tonalité positive ou négative de certaines expériences passées**, de la fonction dans le groupe ». Ainsi, l'évaluation en accord avec les travaux de Short (1984) « est avant tout biaisée par les groupes sociaux légitimés, c'est-à-dire par les institutions impliquées dans les **interactions sociales quotidiennes et ordinaires avec la famille, les amis et les collègues** » (Dake 1992 p. 27). Sur la base de ce constat, Cadet et Kouabenan (2005) évoquent une culture construite du risque, **établie sur les partages d'expériences au sein d'un même groupe le conduisant à des croyances communes**. Pour ces mêmes auteurs, ces biais amènent à la banalisation de certains risques, ou, au contraire, à une surévaluation (op. cit.). Pour étayer ces propos, les auteurs citent deux études portant sur les risques routiers pour la première et sur le risque de contamination pour le personnel soignant pour la seconde. La première étude souligne que les conducteurs expérimentés tendent généralement à sous-évaluer le risque routier, alors que les personnes peu expérimentées le surestiment (Cadet et Kouabenan 2005). La seconde étude établit une conclusion sensiblement différente pour les personnels soignant, dont ceux en contact avec des patients sous-évaluent le risque alors que ceux qui ont été affectés par la contamination le redoutent davantage. Nous pouvons mettre en perspective ce dernier constat de ceux

identifiés dans la littérature SSI, **qui indiquent une sensibilité accrue des top-managers pour la SSI, après que ceux-ci aient rencontré un incident** (Barlette 2012 ; Choobineh et Dhillon 2007 ; Goodhue et Straub 1991 ; Hagen et al. 2008 ; Kotulik et Clark 2004 ; Vance et al. 2014). Cadet et Kouabénan (2005 p. 18) évoquent un parallèle entre les conclusions sur la perception des risques routiers et le risque de contamination des personnels soignant, pour étayer que les top-managers évaluent différemment le risque que « les personnes en position subalterne ». Dans le champ de la SSI, notons que ce parallèle est en accord avec les conclusions d'Albrechtsen et Hovden (2009) qui indiquent un**e différence de perception des risques SI entre utilisateurs et managers**, malgré les efforts de sensibilisation de ces derniers.

Si les individus ne s'accordent pas toujours sur les caractéristiques « matérielles » d'un risque, il apparait que **ces divergences proviennent de la subjectivité liée d'une part au contexte dans lequel le risque est perçu**, présenté comme un déterminant social, d'autre part « aux filtres » de celui qui le perçoit et, enfin, à ses propres enjeux et objectifs (Yates et Stone 1992).

Une fois précisés les suppositions et concepts caractérisant le paradigme psychométrique, nous pouvons prolonger sa description par sa méthode d'évaluation.

L'évaluation psychométrique du risque

Le paradigme psychométrique consiste à recueillir le jugement quantitatif des évaluateurs pour des risques dans un contexte et des activités définis. Il permet de présenter un niveau de risque pour des activités, des substances ou des technologies diverses (Hermand et Chauvin 2008 ; Slovic et al. 1987), en regard des facteurs caractérisant la perception du risque, nommés ci-après « déterminants » (Slovic et al. 1982). Slovic et al. (1987) définissent la méthode de ce paradigme d'étude des risques, comme une mesure et un traitement des données subjectives selon des techniques utilisées en psychométrie (analyse factorielle notamment), pour « produire des représentations quantifiées ou carte cognitive des attitudes et perceptions des risques » (Cadet et Kouabénan 2005 p. 20). Slovic et al. (1984 p. 187) inscrivent cette méthode dans l'objectif de « comprendre et prévoir la façon dont les individus répondent » aux risques à l'appui d'une « taxonomie pouvant expliquer, par exemple, l'aversion extrême des gens à quelques dangers, leur indifférence envers d'autres et les contradictions entre ces réactions et les avis des experts ». À cette fin, Slovic et al. (1979 ; 1982a ; 1982b) établissent dix-huit déterminants de la perception des risques

classés selon trois facteurs : « effroi », « familiarité » et « nombre d'individus exposés ». Il s'agit de questionner les gens sur leur jugement des risques pour, *in fine* qu'ils expriment leur volonté que ces risques soient « régulés » et « réduits » (Slovic et al. 1984 p. 187). Ces choix sont mis en perspective des caractéristiques qualitatives des risques, soit les déterminants, positionnés sur le facteur 1 et 2, telles que par exemple le volontarisme, la maitrise, la connaissance ou la nouveauté, les avantages obtenus pour la société par cette prise de risque, et enfin du nombre potentiel de personnes qui subiraient les dommages liés à ce risque, soit le facteur 3.

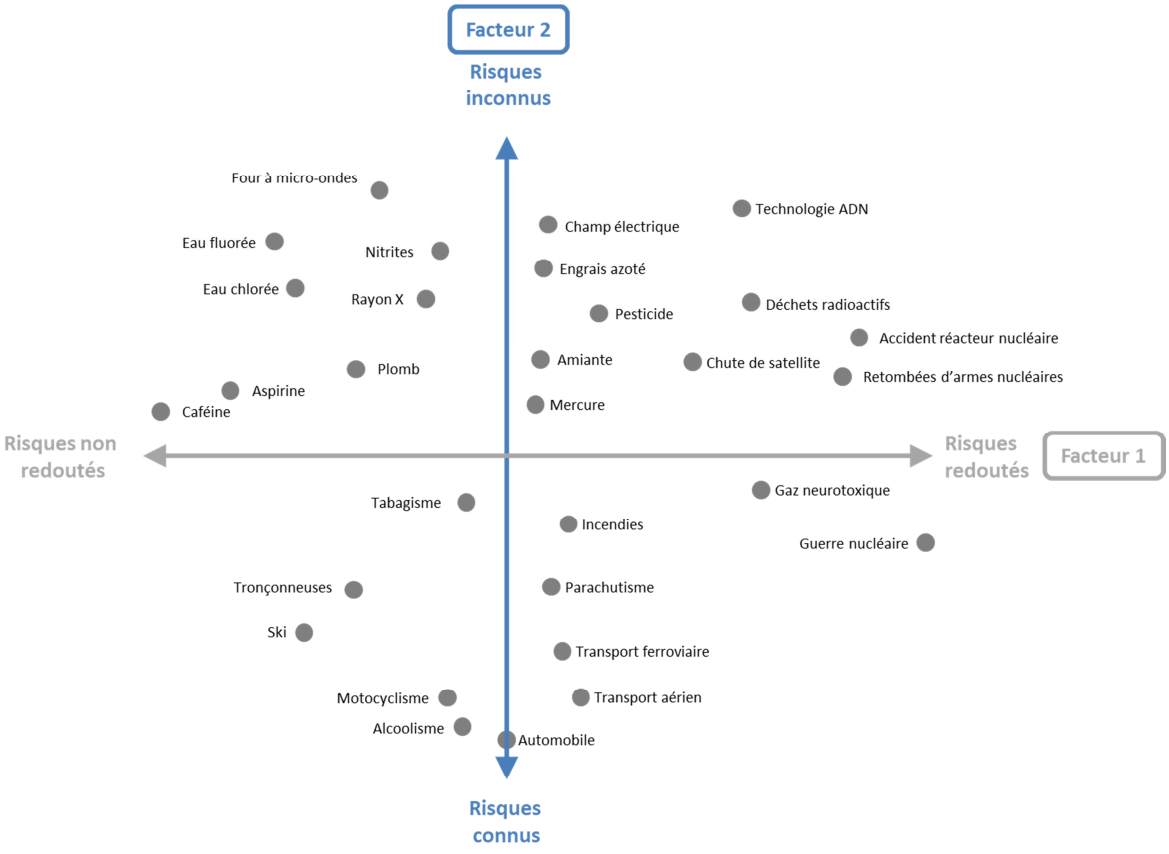


Figure 13.1 : Position des risques selon les 18 déterminants du risque
(adapté de Slovic et al. 1987)

Un consensus, issu de l'ensemble des travaux mobilisant le paradigme de perception des risques, confirme la caractérisation du risque sur les trois facteurs principaux, permettant d'expliquer l'aversion au risque et la volonté de le traiter, tant pour les profanes que pour les experts, quels que soient les risques étudiés (Hermand et Chauvin 2008 ; Kermisch 2010 ;

Slovic et al. 1987). Pour Hermand et Chauvin (2008), les résultats de ces études permettent d'interpréter les perceptions des risques, qui sont directement liées à la position du risque sur l'axe « effroi ». **Plus un risque est jugé effrayant, plus la note attribuée par les évaluateurs est élevée sur le facteur 1, plus ils souhaitent que ce risque soit réduit** (Slovic et al. 1984 ; cf. figure 13.1 et figure 13.2).

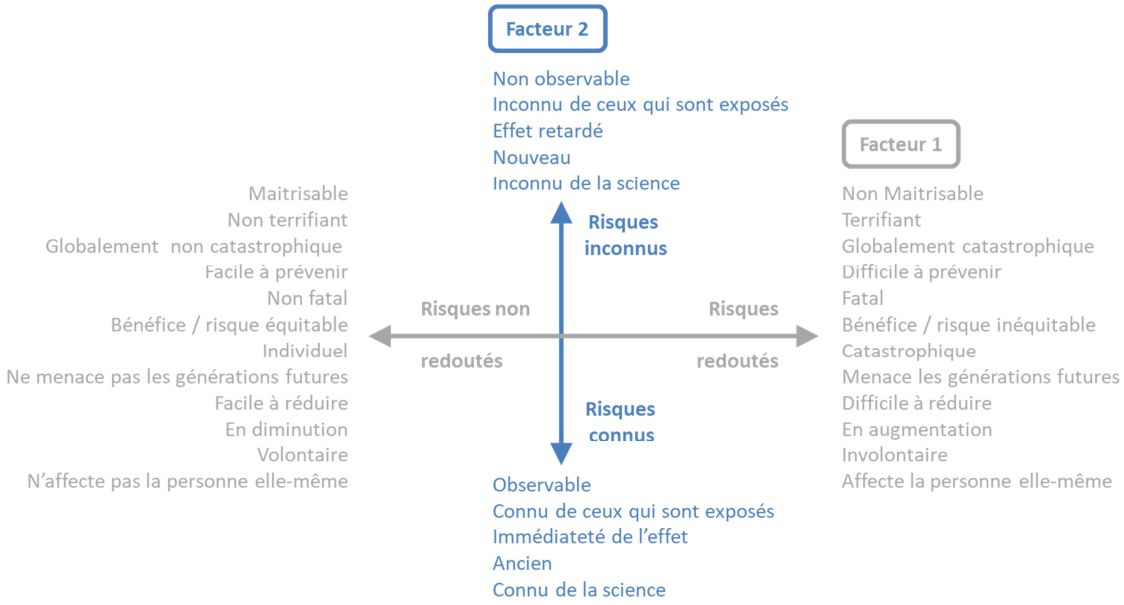


Figure 13.2 : Détail des déterminants sur les deux facteurs

(adapté de Slovic et al. 1987)

Pour Kermisch (2010) et Hermand et Chauvin (2008), les nombreux travaux testant le modèle du paradigme psychométrique mettent en perspective les relations entre les déterminants du risque. En effet, Slovic et al. (1984 p. 188) précisent la corrélation des déterminants l'un avec l'autre, par exemple les risques « évalués comme "volontaires" ont tendance à être notés aussi "contrôlables" et "bien connus" », et les risques « qui menacent des générations futures ont tendance à être aussi vus comme potentiellement catastrophiques ». Précisément, le **facteur 1 révèle le degré de compréhension d'un risque**, autant pour les profanes et que pour les experts (Slovic et al. 1984), et détermine le caractère redoutable ou épouvantable du risque (*dreadful risk*). Il oppose « par exemple les risques liés aux armes nucléaires, aux gaz de combat, au terrorisme et aux actions de guerre, à des risques plus "domestiques" tels l'usage des cosmétiques ou des sèche-cheveux, les bains de soleil, les gazinières, les appareils électroménagers » (Cadet et Kouabénan 2005

p. 19). Le **facteur 2, quant à lui, révèle la familiarité du risque pour l'évaluateur**, ou le degré avec lequel les risques sont perçus comme inconnus et peu familiers. Enfin, le troisième facteur, relatif au nombre de personnes exposées, est qualifié de « moins stable » par Cadet et Kouabénan (2005). L'évaluation de ce facteur ne prendrait pas seulement en compte le nombre de personnes exposées mais également des éléments spécifiques à l'évaluation, tels que par exemple l'affect (cf. « Le risque acceptable » p. 114 dans le paragraphe 3.2.2, Concepts de l'étude des risques).

Les résultats obtenus par ces évaluations psychométriques mettent en perspective l'acceptabilité du risque et particulièrement « des considérations qui affectent le jugement relatif à l'acceptation des risques » (Kermisch 2010 p. 50). Ainsi, Kermisch (op. cit.), sur la base des travaux théoriques de Starr (1969), énonce plusieurs de ces considérations, vérifiées par les résultats empiriques des travaux mobilisant le paradigme psychométrique, telles que par exemple :

- les risques dont les effets sont immédiats sont moins acceptables que les risques pour lesquels les conséquences sont prévues à plus long terme
- les risques connus sont plus acceptables que les risques dont les conséquences ne sont pas connues (vérifiant l'appréhension plus importante pour l'acceptation d'une nouvelle technologie)
- un risque courant est plus acceptable qu'un risque terrifiant, pouvant susciter « des réactions d'horreur ou d'épouvante »
- un risque dont les caractéristiques prévoient des conséquences irréversibles est moins acceptable que lorsqu'il est possible de diminuer les conséquences.

Si les études psychométriques du risque s'attachent préalablement à identifier les caractéristiques perçues du risque, elles sont complétées par l'évaluation des bénéfices, en accord avec les conclusions de plusieurs auteurs (Fischhoff 1979 ; Finucane et al. 2000 ; Kermisch 2010). Rappelons que Slovic et Peters (2006 p. 323) précisent que les individus observent un risque selon des bénéfices attendus alors que Slovic et al. (1982) confirment des conclusions obtenues antérieurement (Slovic et al. 1979), soit que le risque perçu est en relation inverse avec les bénéfices attendus. Cela signifie alors qu'une activité risquée est perçue d'autant moins nocive qu'elle procure plus de bénéfices, conduisant Slovic et al. (1987), à établir qu'une « quantité » subjective de risque nécessite **une « quantité » subjective de bénéfices à la puissance trois** pour que le risque soit potentiellement

acceptable, en accord avec les conclusions de Starr (1969). Précisément, Fischhoff et al. (1978), après avoir interrogé les individus sur les risques liés à plusieurs activités et sur les bénéfices perçus questionnent ces mêmes individus afin d'établir le **facteur d'ajustement** du risque.

Déterminants	Définitions
Facteur 1 : Effroi	
1. Maitrisable	Est-ce que l'occurrence ou les conséquences (dommages) du risque peuvent être contrôlées ?
2. Commun ou terrifiant	Le risque est-il commun ou courant : « les individus ont-ils l'habitude de côtoyer le risque, peuvent-ils penser rationnellement et calmement, ou le risque suscite-t-il une terreur viscérale » (Kermisch 2010 p. 65)
3. Chronique ou catastrophique	Le risque provoque-t-il simultanément un seul décès ou un grand nombre ?
4. Difficile à prévenir	Le risque peut-il être évité ?
5. Fatal	Quelle est la probabilité que le risque soit fatal ?
6. Bénéfice / risque inéquitable	Les risques et bénéfices sont-ils équitablement répartis entre les individus concernés ?
7. Globalement catastrophique	Quel est le niveau d'effroi (nombre de personnes mortes, niveau de dommage matériel) ?
8. Menace les générations futures	Les risques toucheront ils les générations à venir ?
9. Difficile à réduire	Les mesures pour diminuer le risque
10. En augmentation	Le niveau de risque augmente-t-il ou diminue-t-il avec le temps ?
11. Involontaire	Les individus sont-ils engagés volontairement dans la situation à risque ?
12. Affecte la personne elle-même	Les conséquences du risque exposent-elle personnellement l'individu ?
Facteur 2 : Familiarité	
13. Non observable	Les processus conduisant au risque sont-ils identifiables ?
14. Inconnu de ceux qui sont exposés	Quelles sont les connaissances des individus exposés au risque ?
15. Immédiateté de l'effet	Le risque aurait-il des conséquences immédiates ou ultérieures ?
16. Nouveau	Le risque apparait-il, est-il familier ou ancien ?
17. Inconnu de la science	Quel est le niveau de connaissance des scientifiques sur le risque ?
Facteur 3 : Nombre d'individus exposés	
18. Personne exposée	Quel est le nombre de personnes exposées au risque ?

Tableau 5 : Déterminants du risque (Slovic 1982a ; 2000)

Il s'agit pour les individus de se prononcer en regard de chaque risque, sur un des trois ajustements possibles : 1) le risque est acceptable, le niveau de risque pourrait être X fois supérieur ; 2) le niveau de risque est acceptable ; 3) le risque n'est pas acceptable, le niveau de risque doit être X fois inférieur (Kermisch 2010 p. 64). Par exemple, pour le risque perçu lié à l'utilisation de l'énergie nucléaire, le bénéfice perçu est évalué à 52 alors que le risque perçu est évalué à 250, avec un facteur d'ajustement (X) à 32,2. Le risque jugé acceptable est alors évalué en divisant le risque perçu par le facteur d'ajustement soit 250 par 32,2 résultant à environ 8 (plus cette valeur est élevée, plus le risque est jugé acceptable).

Selon Kermisch (2010), ces résultats soulignent la **volonté marquée**, pour les individus, **d'accroitre la sécurité pour chaque risque**, en accord avec les remarques de Cadet et Kouabénan (2005), indiquant que plus le risque est perçu comme important, plus l'ajustement sur le risque acceptable est jugé nécessaire. Ces résultats mettent également en évidence la relation entre l'acceptabilité des risques en perspective des bénéfices perçus, qui, lorsqu'ils sont élevés, impliquent un niveau de risques perçus plus faible, en accord avec les conclusions des études de Slovic et al. (1979 et 1982).

Activité	Bénéfice perçu	Risque perçu	X (individu interrogé sur les risques)	Risque acceptable (individu interrogé sur le risque	X (individu interrogé sur le bénéfice)	Risque acceptable (individu interrogé sur le bénéfice)
1 - Contraceptifs	113	50	2,1	24	1,9	26
2 - Énergie électrique	274	52	1,2	43	0,9	58
3 - Colorants alimentaires	16	31	2,7	11	3,4	9
4 - Appareils électroménagers	133	25	1,1	23	1	25
5 - Véhicules automobiles	187	247	7,3	34	4,9	50
6 - Énergie nucléaire	52	250	32,2	8	25,9	10
7 - Pesticides	87	105	10,5	10	8,5	12
8 - Ski	38	45	1,1	41	1,0	45
9 - Chirurgie	164	104	2,2	47	1,6	65
10 - Rayons X	156	45	2,1	21	1,3	35

Tableau 6 : Résultats partiels des risques perçus et bénéfices perçus
(adapté de Kermisch, 2010 p. 61, sur la base des travaux de Fischoff et al., 1978)

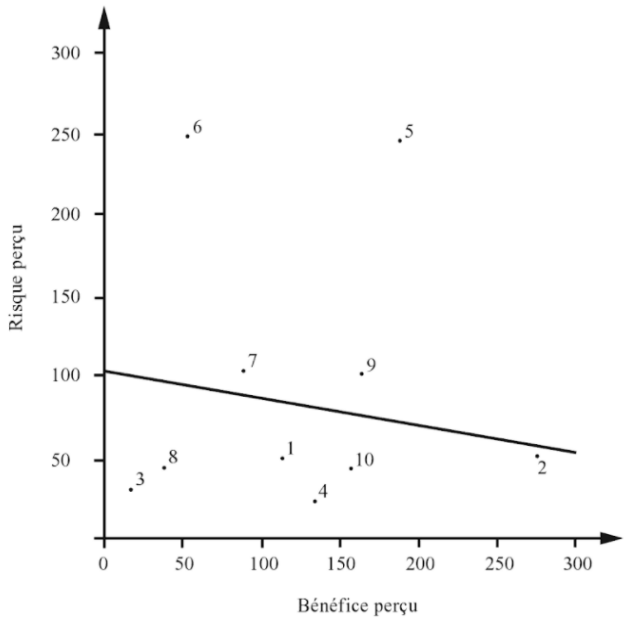


Figure 14 : Résultats partiels des relations entre risques perçus et bénéfices perçus
(adapté de Kermisch, 2010 p. 62, sur la base des travaux de Fischoff et al., 1978, les valeurs numériques renvoient aux activités du tableau 6)

Après plusieurs décennies de recherche sur la perception des risques, le paradigme psychométrique semble offrir une explication fiable sur la différence de perception des risques pour certaines activités, substances, ou technologies, entre experts et profanes et entre des groupes d'appartenance des évaluateurs (Cadet et Kouabénan 2005 ; Hermand et Chauvin 2008 ; Kermisch 2010).

Conçue par Slovic, Fischhoff et Lichtenstein (1979 ; 1980 ; 1987), la littérature fait consensus sur les apports, mais également sur les faiblesses de cette méthode.

En termes d'apports théoriques, le risque est conceptualisé comme un construit défini par des facteurs psychologiques et sociaux, basés sur de multiples déterminants subjectifs (Hermand et Chauvin 2008 ; Kermisch 2010 ; Slovic et al. 1987). Dans ce cadre, l'évaluation du risque relève alors d'une activité complexe pour laquelle l'évaluateur est conduit à caractériser la situation et apprécier les effets impliquant « l'utilisation de valeurs personnelles ou sociales » (Cadet et Kouabénan 2005 p. 20). En termes d'apports méthodologiques, le paradigme psychométrique a démontré la possible généralisation de résultats en mesurant « de façon quantitative les opinions complexes et subtiles d'individus

profanes sur les risques » (Hermand et Chauvin 2008 p. 354). En ce sens Cadet et Kouabénan (2005 p. 20) soulignent « la richesse et les qualités de précision et de fidélité des évaluations subjectives ». Particulièrement les travaux à l'appui de la méthode d'évaluation du paradigme psychométrique établissent des conclusions convergentes soulignant « que le risque perçu était quantifiable et prédictible » (Hermand et Chauvin 2008 p. 357).

Ces caractéristiques, selon Slovic (1982b), mettent en perspective un apport majeur pour l'évaluation des risques, **la mesure du risque acceptable**. En effet, outre l'évaluation, l'objectif visé par le paradigme psychométrique était de comprendre les attitudes individuelles et sociales envers les risques auxquels les êtres humains sont confrontés (Slovic 1999). Les études mobilisant le paradigme psychométrique font émerger une différence d'évaluation du risque entre experts et profanes, accentuant les apports du concept de déterminants, mobilisés pour la perception des risques. Il apparait ainsi pour certain risques létaux que les experts appuient leur évaluation en termes quantitatif, soit le nombre potentiel de morts, alors que les profanes considèrent les caractéristiques qualitatives, soit les 18 déterminants définis par Slovic et al. (1987) et le bénéfice perçu pour l'activité potentiellement mortelle. Également, selon Cadet et Kouabénan (2005 p. 27) l'étude de deux groupes a permis de mettre en évidence que le groupes des experts n'attribuent pas des importances équivalentes aux mêmes informations dans la même situation que le groupe des profanes. Ainsi, le paradigme psychométrique met en évidence la prévalence de ces déterminants dans la perception des risques. Par exemple, si des désaccords sur le niveau global de risque peuvent être observés entre deux groupes d'individus, les déterminants mobilisés pour évaluer ce risque sont convergents (Kermisch 2010).

À contre-pied d'un « risque acceptable universel » ce paradigme permet de personnaliser le risque, soit d'en rendre compte sous la forme **d'une décision individuelle** parmi plusieurs choix, afin de rendre le risque acceptable (Slovic et al. 1984). Précisément, **ce choix parmi les alternatives**, dépend de l'ensemble d'options, des conséquences, des valeurs et des faits invoqués dans le processus de prise de décision » (Slovic et al. 1984 p. 197). Ainsi, **cette méthode d'étude des risques perçus s'inscrit de façon pertinente à l'appui de nos travaux** car elle permet d'individualiser la décision, soit l'acceptation du risque, en fonction de la représentation personnelle de ses déterminants. En effet, notre projet vise à explorer les influences sur l'adoption symbolique de la SSI, dont nous rappelons que l'essence est justement la gestion des risques. En ce sens, le paradigme psychométrique peut permettre la mise en perspective des déterminants pris en compte individuellement dans la perception

du risque SI et du risque acceptable, par les top-managers, conduisant à la possible décision d'ajuster le risque (Slovic et al. 1979 et 1982), soit de mettre en œuvre un niveau de sécurité accru pour la situation potentiellement risquée (Kermisch 2010 ; Cadet et Kouabénan 2005). Rappelons que ce choix dépend de l'ensemble d'options, des conséquences, des valeurs et des faits invoqués dans le processus de prise de décisions (Fischhoff et al. 1981).

Une des premières limites de ce paradigme est énoncée par Slovic (1992) lui-même et directement en lien avec l'apport énoncé ci-avant. Slovic s'interroge sur la rationalité de l'individu, en accord avec les travaux de Starr (1969) et de leur éclairage sur la préférence des évaluateurs. En effet, à l'instar du paradigme de l'utilité espérée, duquel est issu le paradigme psychométrique (Slovic et al. 1985), il est établi sur un fonctionnement rationnel de l'évaluateur (Cadet et Kouabénan 2005). Ce paradigme met alors en évidence des perceptions et des préférences exprimées, supposant que les individus peuvent fournir des réponses rationnelles à des questions difficiles, sinon impossibles, telles que par exemple celle posée par Slovic (1992 p. 5) « quel est le risque de mort aux États-Unis associé au nucléaire ? ». L'évaluation tient compte non pas seulement des caractéristiques du risque mais des conséquences de la situation risquée et des bénéfices (Kermisch 2011). La décision d'accepter un risque repose alors sur une combinaison de règles complexes pour une variété de conséquences sur lesquels le paradigme psychométrique est silencieux. En d'autres termes, la capacité de l'évaluateur à combiner ces règles complexes et à accéder à l'ensemble des conséquences n'est pas certaine (Slovic et al. 1979 ; Yates et Stones 1992). Dans le champ de la SSI, nous pouvons citer une des conclusions de Goodhue et Straub (1991 p. 22-23) qui soulignent le manque de rationalité attendu le nombre avéré d'incidents de sécurité, en indiquant « l'intérêt pour la sécurité est faible pour beaucoup d'individus » montrant alors que « la préoccupation pour **la sécurité n'est pas adossée à des bases rationnelles** ». Notons également que les travaux d'Albrechtsen et Hovden (2009) soulignent l'importance des conséquences potentielles des risques SI sur l'activité des utilisateurs qui seraient impactés indiquant « que les utilisateurs sont plus égocentriques dans leurs évaluations et associent le risque avec **les conséquences immédiates pour eux** si quelque chose dysfonctionne ». Enfin, Les risques peuvent être déterminés par les individus en regard des conséquences possibles pour d'autres, et que le risque est davantage observé sous l'angle des conséquences négatives, en accord avec les conclusions de Bandyopadhyay et al. (1999) et Yates et Stones (1992) et à l'inverse des avantages portés par la situation risquée tels que définie par Slovic et al. (1982a).

La capacité limitée des évaluateurs, soulignée par Slovic (1992) comme faiblesse du paradigme psychométrique, mérite une attention particulière. Rappelons que le paradigme psychométrique relève de la mesure de l'acceptation des risques sociétaux, dont Slovic et al. (1979, 1982, 1987) ont défini les déterminants. Nos travaux ne visent pas à définir un modèle permettant d'identifier et de généraliser les combinaisons des déterminants conditionnant l'adoption ou le rejet de la SSI. Nous retenons davantage le paradigme psychométrique comme une méthode qui, selon Slovic (1984 p. 196), permet d'une part de « caractériser les fonctions essentielles des problèmes de risque acceptable » et d'autre part de créer une taxonomie des déterminants mobilisés « pour la prise de décisions » en articulant risque/profit et coût/profit. En d'autres termes, nous mobilisons les méthodes d'évaluation des risques perçus, appliquées à la gestion du risque SI, en explorant quelles influences sont considérées dans la décision d'adopter symboliquement la SSI

La seconde limite du paradigme psychométrique, énoncée par plusieurs auteurs, prend source dans la critique sur les approches cognitives du risque (Cadet et Kouabénan 2005 ; Douglas et Wildavsky 1983 ; Rippl 2002 ; Sjöberg et al. 2004). Ainsi, dans le prolongement de l'absence de certitude sur la rationalité de l'évaluation, évoquée ci-avant, Douglas et Wildavsky (1983) soulignent le manque de considération de « l'influence sociale et culturelle, comme si l'individu était régi par un fonctionnement purement solipsiste et utilitariste » (Le Breton 2012 p. 24-25). Selon ces auteurs, le risque ne serait alors pas évalué sur les seuls déterminants mobilisés par l'individu, mais en tenant compte des représentations sociales, des connaissances et évaluations partagées par les membres d'un groupe social. Les travaux de Douglas et Wildavsky (1983) mettent ainsi en perspective l'importance des sources qui produisent les informations et leur impact sur les évaluations. Rappelons que Sjöberg et al. (2004 p. 10) considère que les influences sociales pouvant modifier l'acceptabilité d'un risque sont intrinsèques au paradigme psychométrique, car justement mobilisé pour identifier et quantifier des facteurs comparés entre groupes d'évaluateurs (Slovic et al. 1980 ; 1987). Afin d'appréhender les influences sociales qui peuvent modifier l'acceptabilité d'un risque, nous développons la théorie culturelle du risque, de Douglas et Wildavsky (1983), dans la section suivante.

La théorie culturelle du risque

Sjöberg et al. (2004 p. 10) : « deux théories distinctes dominent actuellement le champ de perception de risque. Une est "le paradigme psychométrique", enracinée dans les disciplines

de psychologie et des sciences de décision, tandis que l'autre provient de "la théorie culturelle", développée par les sociologues et les anthropologues ». Une des suppositions les plus importantes dans l'approche psychométrique est que le risque est par construction subjectif, caractérisant une différence majeure avec la théorie culturelle du risque (Sjöberg et al. 2004 ; Tansey et O'riordan 1999).

Pour introduire la théorie culturelle du risque nous pouvons citer la synthèse de Rippl (2002) pour qui le paradigme psychométrique a permis de mettre en évidence deux facteurs principaux, l'effroi et l'inconnu. Si Slovic et ses collègues (Slovic al. 1980, 1987, 1992) ont pu modéliser et éprouver une structure du risque à trois facteurs dans différents contextes, « cette approche ne peut pas **expliquer des différences des niveaux de perception de risque parmi des groupes sociaux** et ethniques » (Rippl 2002 p. 147). Pour cette auteure, le paradigme psychométrique est complété par la théorie culturelle du risque, qui permet d'éclairer la perception et de la gestion des risques, en considérant les incertitudes selon les **styles de pensée** qui régissent l'action sociale des individus. En effet, Rippl (2002) identifie des différences, dans plusieurs recherches mobilisant le paradigme psychométrique, ne permettant pas d'expliquer à partir de variables cognitives, pourquoi une technologie donnée effraie un groupe dans un contexte donné alors qu'un autre groupe ne l'est pas. Ce questionnement est au cœur des travaux de Douglas et Wildavsky (1983) sur la théorie culturelle du risque. D'une part, ils s'interrogent sur les raisons conduisant les individus à percevoir comme dangereux des produits et des pratiques définies comme suffisamment sécurisés (Wildavsky et Dake 1990). D'autre part, ils souhaitent identifier les différences entre des individus percevant une technologie comme dangereuse et des individus qui la considèrent comme suffisamment sécurisée (op. cit.). Ainsi, Douglas et Wildavsky (1983) adoptent une position sociologique pour éclairer la perception des risques. Ils affirment que les valeurs et les visions du monde se combinent dans certains contextes sociaux et culturels, autrement appelés « **biais**[42] **culturels** » pour former la perception des risques des individus (Tsohou et al. 2006 p. 202). L'action des individus est justifiée par les croyances et les valeurs partagées par les individus d'un même contexte (Calvez 2006). Les individus sont incorporés dans une structure sociale qui agit, d'une part, comme un filtre et forme leurs valeurs, attitudes et des visions du monde (Rippl 2002). Un des fondements de la théorie culturelle du risque est soulignée par Rippl (2002), à savoir que les membres d'un même

[42] Kermisch (2010) rappelle que le terme « biais » n'est pas négativement connoté mais employé par Mary Douglas comme une approche, contrairement aux biais cognitif de Kahneman et Tversky

groupe ont des perspectives communes qui imposent de façon particulière l'ordre social du groupe sur la réalité (Tansey et O'riordan 1999).

Selon Wildavsky et Dake (1990 p. 166) seule la comparaison des types de danger considérés par chaque individu peut définir les préoccupations à la base de leur perception et l'importance qu'ils y accordent. En ce sens, la théorie culturelle du risque permet d'expliquer quelle sorte d'individu percevra les risques comme bénins ou à l'inverse très « dangereux ». Précisément, Tsohou et al. (2006 p. 202) indiquent que « la façon dont les gens interagissent socialement empiète sur les systèmes de symboles qu'ils utilisent pour comprendre le monde » et que cela constitue « le postulat de base de la théorie culturelle ». Donc, l'utilisation des biais culturels des individus permet de mettre en perspective leur compréhension des alternatives possibles aux risques en regard des contraintes sociales ou des structures auxquelles ils sont exposés. Ainsi, la théorie culturelle fournit des explications sur la façon et les raisons qu'ont les individus de formuler leurs perceptions des risques (Tsohou et al. 2006 p. 202). Précisément, cette théorie dresse un modèle d'analyse culturelle prenant en compte les quatre cadres sociaux, dans lesquels les individus agissent, que sont les institutions **individualistes, hiérarchiques, égalitaires et fatalistes**. Cette typologie correspond à des « principes d'ordre auxquels les individus marquent leur attachement, ils orientent leurs actions, leurs argumentations et leurs justifications » (Calvez 2006 p. 4). Douglas et Wildavsky (1983) ont défini un modèle nommé « grid-group » permettant de positionner les individus dans ces cadres sociaux selon les valeurs communes et les croyances semblables qu'ils partagent. Calvez (2006) précise la relation des individus aux structures et à leur prise en compte dans la représentation du risque mobilisée par Douglas et Wildavsky (1983). Les principes culturels sont partagés dans un groupe donné permettant de justifier les relations que les individus entretiennent avec celui-ci. Ces principes orientent alors la perception des situations nécessitant d'apporter des réponses, pour lesquelles les principes du groupe servent de justifications. Ainsi, le groupe et plus particulièrement la relation de l'individu au groupe, permet d'apporter une explication sociologique aux perceptions, aux représentations et aux logiques argumentaires que les individus mobilisent dans différentes situations sociales (Calvez 2006). La théorie culturelle « ne considère pas la culture comme un système figé qui gouverne les actions des individus en modelant leur personnalité, mais comme un cadre de référence », que les individus « façonnent et transforment au cours de leurs interactions » (Calvez 2006 p. 3).

La théorie culturelle du risque propose de mettre en perspective ce que craignent les individus en regard de leur mode de vie (*way of life*), c'est-à-dire « par rapport "'à la culture"

à laquelle ils appartiennent » (Douglas et Wildavsky 1983 ; Rippl 2002 p. 149). Douglas et Wildavsky (1983) ont développé la typologie de grille/groupe, qui définit quatre modèles prototypiques comportementaux caractéristiques du modèle de relations sociales, accompagnés d'un système cognitif qui inclut des attitudes et des valeurs. Ces quatre modèles sont distribués selon deux dimensions centrales à la société, « grid » et « group » traduisant respectivement le contrôle et l'engagement social[43] (Rippl 2002, cf. figure 15). Selon Tsohou et al. (2006), la dimension grid dénote le niveau de restriction sociale alors que la dimension « groupe » se réfère à la force d'engagement d'un individu dans le groupe social et la force de son adhésion à ses valeurs.

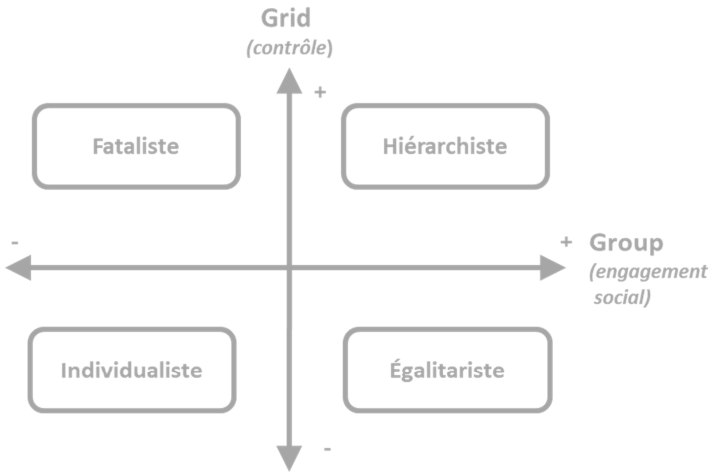


Figure 15 : Typologie des modes de vies selon la théorie culturelle du risque
(Rippl 2002)

Notons que l'approche méthodologique du paradigme psychométrique « se fonde sur l'élaboration et la soumission de questionnaires, ainsi que sur l'analyse de données statistiques » (Kermisch 2010 p. 54), alors que la théorie culturelle du risque présente une nuance. Si Sjöberg et al. (2004) précisent l'utilisation de méthodes statistiques multivariées pour identifier et interpréter les facteurs de réponse de groupe et d'individu, Tsohou et al. (2006 p. 207) mobilisent la théorie culturelle du risque selon l'application d'une méthode qualitative, telle « l'observation de participant et des groupes de discussion ». En effet, selon ces mêmes auteurs deux perspectives ont été appliquées, nommées stabilité et mobilité. La

[43] Kermisch (2010 p. 104) traduit « grid » par « grille des rôles sociaux » et « group » par « incorporation sociale »

perspective de stabilité établit que les individus se conforment à un biais culturel indépendamment du contexte social, permettant d'employer une méthode quantitative pour les identifier (Dake 1992 ; Rippl 2002). À l'opposé, la perspective de mobilité contextualise le biais, soit la capacité pour un individu de « s'attacher aux structures sociales avec les types différents de biais culturels et dans les domaines différents de leurs vies », permettant alors d'adopter des biais différents au fil du temps (Tsohou et al. 2006 p. 203). Ceci permet l'adoption de méthode « comme l'observation de participant et des groupes » dans leur contexte spécifique sur une période établie (op. cit.).

Une fois précisé l'objet de la théorie culturelle du risque, nous pouvons détailler les quatre types, soit hiérarchiste, égalitariste, individualistes et fataliste. Afin d'illustrer chaque biais, nous complétons chacun d'entre eux avec les éléments de langage employés par les individus qui les composent. Ces éléments sont définis dans les travaux de Dake (1992 p. 31) comme échelle partielle du questionnaire sur les biais culturel[44], et repris par Kermisch (2010 p. 182).

Hiérarchiste

Rippl (2002) précise que les hiérarchistes sont des individus dont la vision du monde est caractérisée par des frontières marquées du groupe auquel ils s'identifient sans limite, et par des règles auxquelles il ne faut pas transiger. « La position de ces individus dans le monde est définie par un ensemble de classifications établies, basées sur des critères comme l'âge, le genre, ou la race » (Tsohou et al. 2006 p. 204). Ces démarcations sont considérées incontestables et sont justifiées au motif qu'elles permettent d'adhésion et l'harmonie avec le groupe (Douglas et Wildavsky 1983). Les cultures hiérarchiques soulignent l'importance d'établir et de préserver « l'ordre naturel » de la société. Les hiérarchistes craignent surtout les choses qui perturbent cet ordre social, comme le désordre social, des manifestations, la désobéissance civile et les crimes (Rippl 2002). Une autre caractéristique importante de cette vision du monde consiste en une confiance absolue des dires et des connaissances des experts (Tsohou et al. 2006). En effet, sur la base d'une grande confiance dans les règlements, ces individus croient que l'ordre institutionnel et les experts peuvent traiter tous types de problèmes (Rippl 2002). En ce sens, et particulièrement à la gestion des

[44] L'échelle complète est décrite en annexe « **Biais culturels et éléments de langage** » p. 359 sur la base des travaux de Rippl 2002.

risques, Dake (1992) soulignent que dans cette approche de la société, la conformité aux règlements est censée se décliner du plus haut des institutions jusqu'aux individus. En synthèse, les hiérarchistes sont caractérisés par une faible adaptabilité au changement et une « dépendance excessive à la régularité de leurs façons de faire les choses » (Tsohou et al. 2006 p. 205). Selon Wildavsky et Dake (1990 p. 172) les hiérarchistes, comme les individualistes, sont associés à la prise de risque technologique car ils considèrent davantage le bénéfice potentiel inhérent à la situation risquée qu'à des conséquences éventuellement défavorables.

Éléments de langage permettant d'identifier les individus du groupe **hiérarchiste** (Dake 1992 p. 31) :

- « Nous devrions disposer de forces armées plus puissantes que celles que nous avons »
- « Je pense que la jeunesse devrait faire preuve de davantage de discipline »
- « Je soutiendrais volontiers l'introduction d'un service militaire obligatoire »
- « Les gens devraient être récompensés en fonction de leur position sociale »
- « Je suis plus exigeant que la plupart des gens à propos de ce qui est bien ou mal »

Égalitariste

Si les égalitaristes se positionnent en bas à droite de la grille, ils se caractérisent par un fort positionnement pour le groupe. Contrairement aux hiérarchistes, leurs vies ne sont pas prescrites par la différenciation de rôle (Tsohou et al. 2006). A l'inverse, ils partagent l'idée que les relations aux autres doivent être régies selon chacun et que la position sociale des individus ne définit pas leur autorité hiérarchique (op.cit.). Opposés à ce que d'autres décident pour eux, ils préfèrent baser leurs décisions sur leurs propres informations, permettant alors de faire des choix personnels (Dake 1992). Ainsi, ils remettent en cause la connaissance des experts qu'ils soupçonnent d'être abusivement employée par les autorités. Leur approche de la gestion du risque technologique favorise des résultats centrés sur les dimensions sociales et politiques en élaborant des « hypothèses pour envisager des

problèmes concernant le risque en termes éthiques », critiquant les institutions responsables de la gestion des risques (Dake 1992 p. 29). Wildavsky et Dake (1990 p. 172) ont identifié que les égalitaristes associent « la perception des risques technologiques et environnementaux comme un grave problème pour notre société » et on ainsi une aversion élevée pour ces risques.

Éléments de langage permettant d'identifier les individus du groupe **égalitariste** (Dake 1992 p. 31) :

- « Si les citoyens de ce pays étaient traités de manière plus équitable, nous aurions moins de problèmes »
- « Le gouvernement devrait veiller à ce que chacun ait un bon niveau de vie »
- « Ceux qui sortent du lot devraient être taxés davantage afin d'aider ceux qui sont moins privilégiés »
- « Je serais prêt à soutenir une réforme fiscale qui taxerait davantage les hauts revenus »
- « Je soutiens les efforts du gouvernement pour délivrer le pays de la pauvreté »

Individualiste

Les individualistes sont positionnés selon un engagement social faible sur la grille et un faible contrôle du groupe. Ils se définissent alors selon un principe de liberté, écartant les contraintes artificielles telles que les régulations et les sanctions, permettant à chacun de prospérer, indépendamment des risques qui pourraient impacter les populations (Dake 1992). Ainsi, ni liés au groupe, ni à des rôles stricts, les individualistes affirment que toutes les frontières sont soumises à négociation (Tsohou et al. 2006). Ils craignent principalement ce qui pourrait entraver leur liberté individuelle et réticents pour accepter des règles ou suivre des instructions définies. Rippl (2002 p. 150), en accord avec Dake (1992), souligne que les individualistes « perçoivent les risques comme des opportunités », conduisant par exemple à considérer davantage les nouvelles technologies sous l'angle des possibilités que du danger qu'elles représentent. Selon Dake (1992), les individualistes privilégient les décisions basées sur des jugements personnels plutôt que collectifs, adhérent alors à une stratégie de gestion des risques « dérégulée ». Dans la théorie culturelle du risque, le terme

« individualiste » n'indique pas un individu autonome et libéré de toutes contraintes et contrôles mais plutôt comme agissant selon une approche articulant liberté de négociation dans des systèmes « auto-régulés » définissant des prescriptions contextuelles (Dake 1992 p. 29 ; Tansey et O'riordan 1999).

Éléments de langage permettant d'identifier les individus du groupe **individualiste** (Dake 1992 p. 31) :

- « Dans un système équitable, les individus les plus compétents devraient gagner davantage »
- « Une société libre ne peut exister qu'en donnant la possibilité aux entreprises de prospérer »
- « Les gens qui souhaitent travailler dur devraient avoir droit de le faire »
- « Dans ce pays le plus intelligent devrait être au sommet »
- « Si une personne a réussi à acquérir des richesses, il devrait avoir le droit d'en profiter »

Fataliste

Les fatalistes ont une vision faible du groupe et forte du contrôle, soit une position basse pour le groupe et élevée sur la grille. Les fatalistes se définissent selon une hypothèse qui rationalise l'isolement et la résignation des contrôles rigoureux sur leur comportement. Pour Dake (1992), ils sont ceux qui sont exclus des trois autres types culturels, ne pouvant concourir avec succès sur les marchés, ne pouvant respecter le minimum des normes sociales et ne pouvant rassembler le temps, l'énergie et les ressources exigées pour participer à la vie politique. Comme les hiérarchistes, ils estiment leur autonomie limitée par des distinctions sociales mais n'adhèrent pas aux institutions, auxquelles ils se sentent « étrangers », considérant alors que les règles établies sont éloignées de leurs principes (Tsohou et al. 2006). Les fatalistes prennent part à la vie sociale de plusieurs groupes d'individus restreint en nombre. Si ce que les fatalistes pensent « risqué » est défini par les valeurs et croyances de ces groupes restreints, ils n'en tiennent que peu compte car ils supposent les conséquences inévitables. En ce sens, Kouabénan (2007) et Sjöberg et al. (2004 p. 16) illustrent les comportements des fatalistes qui seraient enclins à prendre « plus de risques et à négliger les mesures de sécurité ».

Éléments de langage permettant d'identifier les individus du groupe **fataliste** (Dake 1992 p. 31) :

- « On se tire plus facilement d'affaire si l'on ne fait confiance à personne »
- « Cela ne sert à rien d'agir pour autrui, à long termes cela nous retombe dessus »
- « La coopération avec les autres fonctionne rarement »
- « L'avenir est trop incertain pour que l'on puisse faire des projets sérieux »
- « J'ai souvent été traité de manière inéquitable »

Perceptions et théorie culturelle des risques

Wildavsky et Dake (1990 p. 167) complètent les travaux de Douglas et Wildavsky (1983) par une approche qualitative de la perception des risques. À la lumière de plusieurs théories, telle que la théorie de la connaissance, de la personnalité, économique et politique, ils démontrent qu'elles ne permettent pas d'expliquer les comportements face au risque. Par exemple, selon eux, la connaissance d'un individu pour une technologie et de ses potentiels risques a « une relation minimale avec la perception de risque » (Wildavsky et Dake 1990 p. 171). Ils indiquent que la perception des risques peut être expliquée par les biais culturels, par exemple, les égalitaires considèrent davantage « les risques technologiques et environnementaux comme un grave problème pour la société et ont alors une forte aversion pour ces activités » (Wildavsky et Dake 1990 p. 172). Enfin, ils concluent que les biais culturels fournissent les éclairages sur la perception et la décision afférente au risque « qui sont plus puissants que les mesures de connaissance de la personnalité » (op. cit).

À l'appui de la théorie culturelle des risques, Sjöberg et al. (2004) émettent un commentaire majeur sur le paradigme psychométrique. Pour ces auteurs, le paradigme est étudié sur le postulat que la perception des risques est fondamentale pour en quantifier son acceptation, soit que plus un risque est élevé, plus les individus souhaitent le réduire. Si ce postulat est qualifié de probable par Sjöberg et al. (2004), ils indiquent toutefois un biais dans cette approche car le paradigme psychométrique **ne prend pas en considération le risque lui-même mais davantage ses conséquences.** Pour étayer leurs propos, Sjöberg et al. (2004

p. 20) soulignent que le « risque d'effroi »[45] a une part « importante du pouvoir explicatif » dans la validité du paradigme psychométrique. Ils concluent que la volonté de réduire les risques, lorsqu'elle est évaluée distinctement du risque, « est plus fortement liée à la **sévérité des conséquences** » et non pas au risque lui-même. Ceci est en accord avec Bandyopadhyay et al. (1999 p. 440), qui, dans le champ de la SSI, précisent que les évaluations de probabilité ne sont généralement pas prises en compte. Ce constat peut être éclairé par les conclusions de Slovic et Peters (2006) qui assurent que les biais de la théorie culturelle, au sens de la typologie, sont des déterminants importants pour le risque perçu. En d'autres termes il s'agit, pour l'évaluateur, de considérer prioritairement l'ampleur des conséquences en regard des croyances de son groupe social, et **non pas les caractéristiques du risque définies par sa probabilité et son impact**.

En complément de ces constats, Sjöberg et al. (2004) indiquent que le paradigme de perception des risques ne mesure pas toujours **directement le risque perçu pour l'individu** interrogé, mais la projection de ce risque par l'individu à d'autres. Ainsi, le risque personnel et le risque général diffèrent dans les études empiriques (Sjöberg et al. 2004). Ce point est central dans l'étude du risque perçu car le risque général émergerait davantage que le risque pour l'individu lui-même, conduisant alors à la mise en place de mesures de sécurité qui s'imposeraient à d'autres et pas nécessairement à l'individu lui-même (Sjöberg et al. 2004). Ils indiquent toutefois que certains risques sont principalement centrés sur les conséquences pour les individus eux-mêmes, dans le cas, par exemple, des habitations exposées aux risques nucléaires.

Dans le champ de la littérature SSI, les travaux de Tsohou et al. (2006) visent l'examen de la perception des risques SI et leur effet sur les stratégies de gestion en regard de la théorie culturelle du risque. Ils postulent que la « théorie culturelle a largement été appliquée dans des études de perception de risque » et soutiennent que les influences sur les risques perçus sont enracinées dans le contexte social ». Précisément les individus peuvent se « conformer à des biais culturels différents selon des contextes spécifiques », justifiant alors de mobiliser la théorie culturelle pour leur travaux (Tsohou et al. 2006 p. 207). Rappelons que ces travaux sont parmi les huit travaux académiques que nous avons identifiés dans la littérature SSI, qui combinent perception des risques et sécurité de l'information (cf. « 3.2.7 Perception des risques et SSI » p. 165). Il nous apparait alors opportun d'en préciser les

[45] Le facteur « effroi » se confond avec le déterminant « catastrophique », le facteur effroi comportant lui-même le déterminant catastrophique (cf. 3.2.5 « Paradigme psychométrique », section « L'évaluation psychométrique du risque » p. 126)

principaux apports, sous forme d'une combinaison des étapes de gestion des risques, en accord avec les travaux de Straub et Welke (1998), de l'initialisation de la méthode, à l'analyse des risques pris en compte et enfin à leur traitement, selon chacun des quatre biais culturels.

Biais culturel	**Choix de la méthode**	**Influence sur l'analyse de risque**	**Influence des options de traitement sur les parties prenantes**
Hiérarchiste	La méthode doit être basée sur les décisions d'expert et les standards de sécurité	Les hiérarchistes considèrent les menaces qui peuvent porter conséquence sur l'ordre social	Les mesures ne doivent pas remettre en cause le cadre de travail
Égalitariste	La méthode doit encourager la participation des parties prenantes	Les menaces sont considérées : – sous l'angle de l'équité[46] – en cherchant l'exhaustivité des informations pour réaliser leur propre analyse	Une résistance à la mise en œuvre des mesures est attendue des parties prenantes ; il est nécessaire de leur expliquer la justification de chaque mesure
Individualiste	La méthode est basée sur le coût / bénéfice du risque	Les menaces considérées sont ceux qui peuvent porter atteinte aux libertés individuelles et ceux dont le coût des conséquences est le plus élevé	Les parties prenantes seront a priori peu disposées à accepter les mesures ; les aspects économiques des mesures doivent être mis en avant
Fataliste	Aucune préférence de méthode attendue que les fatalistes acceptent ce qui leur est imposé	Les menaces prises en compte sont les plus significatifs car considérés comme inévitables	Les mesures doivent pouvoir être des routines dans l'activité quotidienne des parties prenantes

[46] Tsohou et al. (2006) citent en exemple un déni de service comme risque pouvant porter atteinte à l'équité, soit l'impossibilité de continuer à fonctionner normalement pour l'entreprise ciblée

Tableau 7 : Éléments clés des stratégies de gestion des risques SI

(Tsohou et al. 2006 p. 213)

Si l'objectif initial de Tsohou et al. (2006 p. 198) était d'utiliser la théorie culturelle « pour identifier des modèles de perception des risques des parties prenantes et leurs effets sur la gestion des risques du système d'information », il semblerait davantage qu'ils aient mis en évidence « le rôle que les biais culturels jouent » sur les méthodes de gestion des risques SI en regard des aversions catégorisées par cadre social (Tsohou et al. 2006 p. 214). Ainsi, dans leurs travaux n'apparaissent pas les risques SI redoutés, éléments fondamentaux pris en compte dans le modèle de gestion des risques que Tsohou et al. (2006 p. 199) mobilisent.

En conclusion de la théorie culturelle du risque, nous pouvons citer Tansey et O'riordan (1999 p. 72), qui précisent, dans le champ de la santé, « que les points de vue de l'expertise, de l'intégrité scientifique, de la fiabilité professionnelle et de la crédibilité de messages seront tous influencés par **le contexte interactionnel dans lequel les jugements sont réalisés** ».

Synthèse du paradigme psychométrique et de la théorie culturelle du risque

Notre propos n'est pas de confronter les hypothèses et amendements de ces experts académiques sur le paradigme psychométrique et la théorie culturelle du risque. Notre objectif est de préciser ce champ théorique afin d'identifier comment les décideurs perçoivent les risques SI et l'influence de ces risques sur l'adoption symbolique de la SSI. Si le paradigme psychométrique et la théorie culturelle du risque offrent des approches pertinentes sur la caractérisation du risque, ils renforcent davantage notre questionnement sur les risques potentiellement considérés lors de la décision d'adopter symboliquement la SSI et permettent d'appréhender les influences conduisant à l'acceptation du risque.

Un des consensus sur le risque relève de ses multiples dimensions, considérant les incertitudes sur les signes le caractérisant (Yates et Stone 1992), les incertitudes sur la probabilité de survenance (Bandyopadhyay et al. 1999 ; Hermand et Chauvin 2008 ; Yates et Stone 1992), les incertitudes sur les pertes potentielles (Hagen et al. 2008 ; Kermisch 2012) et l'évolution de la situation risquée (Cadet et Kouabenan 2005). Ainsi, **« le paradigme psychométrique est une approche pour identifier les caractéristiques influençant la perception de risque des individus** » (Sjöberg et al. 2004 p. 25), postulant que tous les

individus évaluent le risque de la même manière. La théorie culturelle du risque, en prenant le contre-pied de cette approche, permet alors de compléter le paradigme de perception des risques en introduisant comment **les facteurs sociaux, culturels et institutionnels qui influent sur la réflexion des individus évaluant les risques** (Rippl 2002 ; Sjöberg et al. 2004).

En perspective de la littérature SSI, le paradigme psychométrique et la théorie culturelle du risque présentent des principes parallèles. En effet, la SSI pose comme étape fondamentale l'analyse de risque, première brique du dispositif de sécurité des systèmes d'information. Elle permet d'objectiver les risques, menaces, probabilités et conséquences, conduisant ensuite à une prise de décision sur l'acceptation du risque, après éventuelle réduction, autrement nommées mesures de sécurité dans le champ de la SSI. Si l'étape d'analyse de risque est appelée par la mise en œuvre de la SSI, nous nous interrogeons sur les risques analysés en amont de l'adoption de la SSI et de l'analyse formelle des risques, à minima les conséquences indésirables considérées **pour justement initier la SSI** comme une réponse au risque, afin de le rendre acceptable. Rappelons que, dans le champ de la SSI, seule une analyse formelle des risques permet de décider si le risque doit être traité, transféré, accepté ou si l'activité risquée doit être évitée (ISO 27001 2013) permettant alors de structurer le dispositif de protection des SI de l'organisation.

Tant dans les travaux mobilisant le paradigme psychométrique que la théorie culturelle du risque, la conséquence du risque est considérée comme un facteur majeur dans l'explication de l'attitude, les avantages liés à la situation risquée étant beaucoup moins importants (Sjöberg et al. 2004). Aussi, les conséquences explorées dans ces champs théoriques, font l'objet d'un questionnement spécifique et mature, tel que par exemple le nombre de victimes potentielles d'un accident nucléaire ou encore les études statistique d'accidentologie (telles que les accidents routiers étudiés par Cadet et Kouabénan, 2005). Si ces conséquences sont mises en perspective pour identifier l'acceptation du risque sociétal par les individus et étudiées empiriquement, à notre connaissance, il n'existe pas de travaux comparables sur les risque SI. En effet, d'une part l'étude la discipline de la SSI est apparue au début des années 90 après que les SI soient devenus centraux pour les organisations (Bharadwaj et al. 2013 ; Kayworth et Whitten 2010). D'autre part, les conséquences des risques SI n'ont pas de matérialité comparable à celles des risques sociétaux car les processus sont digitalisés et engagent moins les conséquences humaines. Ce point a peut-être orienté les recherches SSI à considérer les dysfonctionnements du SI sous l'angle technique (Dhillon et Backhouse 2001 ; Kankanhalli et al. 2003 ; Kwon et Johnson 2014). Enfin, en regard des observations de

plusieurs travaux (Fischoff et al. 1978 ; Slovic et al. 1979 ; Starr 1969), selon lesquels une activité doit représenter un bénéfice subjectif à la puissance trois par rapport au risque, ou encore trois fois le bénéfice pour des risques mesurés (Slovic et al. 1987 ; Slovic et Peters 2006), émergent deux questions en accord avec notre problématique. En effet, nous nous interrogeons sur l'étude du rapport risque / bénéfice réalisé par les top-managers pour accepter les risques et également sur les risques SI considérés dans cette évaluation. Dans ce cadre, rappelons que l'activité risquée n'est pas le SI lui-même mais l'usage du SI sans dispositif de sécurité. En transposant les principes du paradigme psychométrique, l'évaluation de l'activité risquée concernerait le SI en l'absence de SSI et l'acceptation concernerait le bénéfice perçu, ou l'absence d'engagement et de ressources nécessaires, pour disposer d'une protection du SI. En effet, Slovic et al. (1979, 1982) précisent que plus le **risque est perçu comme important**, plus les mesures pour le rendre acceptable **sont jugées nécessaires.** Dans nos travaux il s'agit d'étudier justement quels risques sont considérés et comment la décision d'adopter symboliquement la SSI est réalisée, soit en identifiant les bénéfices perçus à protéger le SI et comment elle permet de contribuer à l'acceptation des risques. Rappelons qu'Alhakami et Slovic (1994) mettent en évidence une relation spécifique entre **risque et bénéfice, soit l'affect** (cf. « Le risque acceptable » p. 114), les conduisant à remettre en cause la distinction stricte, jusqu'alors sous-tendue dans les études du risque perçu, soit entre le risque et le bénéfice. Ces mêmes auteurs en déduisent une confusion du risque et du bénéfice par les individus qui procèdent davantage à « une évaluation globale de l'activité » (Kermisch 2010 p. 63) plutôt qu'à une évaluation isolée des deux concepts. En accord avec Alhakami et Slovic (1994), Kermisch (2010) souligne la recherche d'une cohérence de l'évaluation par les individus, telle que considérer comme moins risquée une activité dont les bénéfices sont élevés en regard de la même activité avec des bénéfices moindres. Ces constats renforcent l'individualisation des risques pour des activités et des organisations spécifiques (Dhillon et Torkzadeh 2006), en observant le décideur dans son contexte, nécessitant alors une exploration avancée des caractéristiques et de la nature des risques considérés.

Pour Kermisch (2010 p. 50) le paradigme psychométrique permet de mettre en perspective l'acceptabilité du risque et particulièrement « des considérations qui affectent le jugement relatif à l'acceptation des risques ». Ainsi, nous retenons les caractéristiques principales du risque et de son acceptation, que nous synthétisons ci-après, soit la dimension et construction sociales du risque, l'évaluation du risque et, enfin, l'acceptation du risque.

La **dimension et la construction sociales du risque** relèvent des caractéristiques mêmes du risque que Slovic (1992 p. 5) définit comme subjectif et qui « n'existe pas "ailleurs", indépendamment de nos esprits et cultures ». En effet, la perception d'un risque est individuelle, basée sur les **connaissances personnelles d'une situation spécifique** (Cadet Kouabénan 2005 ; Slovic et al. 1979), relevant des valeurs, des symboles, de l'histoire et l'idéologie (Sjöberg et al. 2004). Si l'accent est mis sur **les connaissances techniques et les expériences passées**, l'évaluation est influencée par le groupe social qui interagit quotidiennement avec l'évaluateur (Dake 1992). Cadet et Kouabénan (2005) prolonge ce constat en indiquant que ces interactions contribuent à l'élaboration d'une culture commune du risque. En effet l'**appartenance au groupe** est mise en évidence par Douglas et Wildavsky (1982) pour qui les perceptions et les évaluations de risques sont réalisées autour de croyances, de valeurs et attitudes communes. En ce sens, Short (1984) souligne la médiatisation de l'information provenant de **plusieurs sources de référence** mettant davantage en perspective les influences sur les représentations sociales du risque. Cadet et Kouabénan (2005) prolongent ce constat en invoquant des groupes ayant une activité risquée ou des caractéristiques semblables telles que par exemple des groupes professionnels ou des fumeurs.

Selon Slovic, **l'évaluation** repose sur des inférences fondées à l'appui d'indices de sources différentes, tels que **les souvenirs, l'expérience d'une situation comparable ou ce qui a été entendu et observé sur** le risque lui-même (Cadet Kouabénan 2005 ; Slovic et al.1979). Rappelons que l'évaluation vise avant tout à définir, pour des activités, des substances ou des technologies diverses, la mesure du risque acceptable (Hermand et Chauvin 2008 ; Slovic et al. 1987). S'il s'agit d'un processus considérant des opinions complexes et subjectives des individus pour lesquels, dans le champ des risques sociétaux, ont été défini « 18 déterminants » (Slovic et al. 1982) permettant de les caractériser et de les comparer. En effet, l'objet du paradigme psychométrique est d'identifier les caractéristiques individuelles et sociales pour les risques. Cette approche a permis, notamment, de comprendre la volonté de réduire certains risques sociétaux, en mettant en évidence plusieurs déterminants tels que la méconnaissance, l'immédiateté, l'ampleur et la réversibilité des conséquences (Kermisch 2010). La prégnance de ces déterminants, dans le paradigme psychométrique, renforce le constat de Slovic et al. (1984) pour lequel les individus souhaitent que les risques définis selon ces déterminants soient réduits. Yates et Stone (1992) éclairent les divergences d'évaluation entre individus dont la subjectivité liée au contexte ne permet pas toujours

d'accéder à une évaluation commune. En effet, outre les indices dont nous avons rappelé l'interprétation subjective ci-avant, l'évaluation peut être assortie d'éléments situationnels dans lesquels se combinent les enjeux et objectifs des évaluateurs (Sjöberg et al. 2004).

L'**acceptation du risque** ne se définit pas par la seule objectivation des conséquences défavorables inhérentes et potentielles de la situation risquée mais, également, à une représentation de ce risque construite sur des choix sociaux. Un risque acceptable devient alors une valeur intermédiaire de référence entre avantages et conséquences négatives (Fischoff et al. 1981). L'acceptabilité repose alors sur plusieurs déterminants développés par Slovic et al. (1979, 1982, 1987), tels que par exemple les connaissances scientifiques, la législation, les expériences, la responsabilité vis-à-vis du risque, la profession exercée et aussi, selon Cadet et Kouabénan (2005), les mesures de sécurité préventives effectives. Enfin, l'acceptation du risque est individuelle car elle s'établit sur des règles complexes combinées à des conséquences multiples dont la connaissance et l'ampleur sont particulières à chaque évaluateur (Slovic et al. 1979 ; Yates et Stones 1992). Si les bénéfices sont mis en perspective lors de l'évaluation, les conséquences négatives sont davantage mobilisées par les individus afin de déterminer si un risque est acceptable. Rappelons que la méthode employée par Fischoff et al. (1978) et Slovic et al. (1979 et 1982) permet de mesurer l'acceptation du risque en interrogeant les individus dans un premier temps sur le risque brut, ne tenant pas compte des bénéfices attendus, et, dans un second temps sur le même risque avec ses bénéfices attendus (cf. Tableau 6 : Résultats partiels des risques perçus et bénéfices perçus). Rappelons également que les travaux de Finucane et al. (2000) puis de Slovic et Peters (2006) complètent le paradigme psychométrique par l'heuristique d'affect, dont l'importance des caractéristiques sont particulièrement influentes dans l'évaluation de situations fortement recherchées ou fortement redoutées, soit en regard des bénéfices « espérés ». **Ces commentaires peuvent porter un éclairage nouveau sur les constats énoncés par les auteurs en SSI**. En effet, si les bénéfices liés à l'activité risquée, soit le SI, sont établis, Straub (1990) souligne justement que les bénéfices de la SSI ne seraient pas quantifiables. Abrams et Bailey (1995) prolongent cette perspective en indiquant que les analyses coûts et bénéfices ne sont pas toujours possibles. Précisément nous avons évoqué l'intangibilité des bénéfices de la SSI dont Hu et al. (2007 p. 166) soulignent, justement, qu'une sécurité réussie se traduit par l'absence de conséquence. Ainsi, d'une part est établi que les bénéfices attendus sont prégnants dans l'acceptation des risques, et d'autre part, dans le champ académique de la SSI, les bénéfices attendus par la couverture des risques seraient difficiles à évaluer. Ceci est convergent avec les travaux de

Straub (1990) qui évoque une possible perception erronée des risques SI par les top-managers et ensuite Straub et Welke (1998) qui constatent une information parcellaire et non exhaustives sur la nature des risques SI auxquels leur organisation est exposée.

Nous pouvons mettre en perspective les travaux de l'acceptation du risque, formulés par le paradigme psychométrique, en regard des constats établis dans le champ de la SSI. D'une part la **connaissance des risques SI serait subjective et propre aux top-managers**, basée sur leurs croyances et les valeurs partagées avec leur réseau d'influence. D'autre part les **bénéfices liés à la SSI sont difficiles à quantifier par les top-managers**, soulevant alors la question de l'intérêt de l'adopter. Rappelons que l'impossibilité d'évaluer les risques SI, selon leurs coûts et bénéfices pourrait *in fine* conduire à ne pas considérer la SSI (Straub et Welke 1998). Enfin, la volonté de réduire le risque est davantage marquée, dans l'évaluation sociétale, pour les risques les plus catastrophiques, suggérant que ceux dont les conséquences sont moins importantes n'appellent pas systématiquement à être couverts. Cette perspective est en accord avec la nécessité de rencontrer un incident SI majeur, provoquant des impacts conséquents, pour que la SSI deviennent une préoccupation des directions générales (Goodhue et Straub 1991 ; Hu et al. 2007 ; Wood 1995). En effet, l'objectivation des conséquences, et donc du risque, provoquée par l'exposition directes des top-managers aux conséquences, peut modifier leurs croyances et ainsi remettre en cause la perception d'une faible exposition des SI aux risques (Barlette et Fomin 2010 ; Kankanhalli et al. 2003). Slovic et al. (1982b) soulignent justement que la majeure partie de la connaissance des évaluateurs provient justement de stimulus, de signaux et d'images dont la valeur a été produite par des évènements perçus comme dangereux. Nous pouvons compléter ces constats par la remarque de Tsohou et al. (2006), qui souligne la différence de perception des risques entre profanes et spécialistes en sécurité des SI, les premiers disposant de connaissance sur le risque SI en regard de l'expérience des seconds.

Après avoir dressé les concepts mobilisés des trois paradigmes d'étude du risque, soit l'utilité espérée, le paradigme cognitif, le paradigme cognitif psychométrique et son complément, la théorie culturelle du risque, nous avons précisé les apports pour notre étude. Précisément, le risque n'est pas universel mais repose sur l'appréciation de l'incertitude, des conséquences et de l'intérêt pour la situation risquée. En effet, d'une part, la subjectivité du concept de risque met en évidence les divergences sur la perception. D'autre part l'évaluation du risque est réalisée selon la connaissance de l'évaluateur et des influences issues de son appartenance à des groupes sociaux. Enfin, l'acceptabilité fait

interagir plusieurs spécificités de l'évaluateur et du risque telles que l'appétence au risque, les bénéfices perçus, le contexte et les enjeux de la situation risquée.

Les caractéristiques, l'évaluation et l'acceptation du risque peuvent éclairer l'adoption symbolique de la SSI, en regard de la littérature de ce champ, qui précise qu'il s'agit d'une activité de gestion des risques SI. Afin de parachever la présentation de la perception des risques dans le champ psychologique, nous nous intéressons aux éléments qui « peuvent potentiellement se trouver impliqués dans l'évaluation des risques », qui se trouvent « à chaque occasion dans une direction toujours identique » soit les **biais d'évaluation** (Cadet et Kouabénan 2005 p. 30)

3.2.6. Les biais d'évaluation des risques

Selon Kermisch (2010) plusieurs biais influencent la perception des risques lorsqu'il s'agit de les évaluer par heuristiques. Ainsi la disponibilité, la représentativité, l'ancrage ajustement, les effets de cadrage de présentation, l'excès de confiance, la persistance des opinions et les erreurs de prédiction peuvent offrir une explication sur la façon dont sont perçus les risques par les individus. Ainsi Cadet et Kouabénan (2005) les individus optent généralement pour une évaluation par heuristiques. En effet, « le jugement stochastique est une activité difficile à réaliser parce que la situation à traiter est souvent complexe et que les capacités de l'opérateur sont limitées » alors que l'évaluation par heuristique est un procédé cognitif de jugement réalisé rapidement en mobilisant une charge cognitive faible (Amalberti 1996 ; Hermand et Chauvin 2008 ; Cadet et Kouabénan 2005).

Les paragraphes suivants présentent les biais les plus importants pour la perception des risque, tant pour les paradigmes d'évaluation des risques basés sur des heuristiques tels que le paradigme cognitif que les biais identifiés lors des études sur le paradigme psychométrique.

Disponibilité

Lichtenstein et al. (1978) à l'appui des travaux de Tversky and Kahneman (1974), soutiennent que les individus estiment la probabilité de survenance d'un risque selon la facilité avec laquelle des situations comparables peuvent être recouvrées de leur mémoire ou imaginées. Ainsi, pour « les événements mortels, le concept de disponibilité suggère que ses jugements soient influencés non seulement par l'expérience directe avec l'exposition

mortelle et indirecte via des films, des livres, la télévision, des journaux, … mais aussi selon les caractéristiques mémorables des causes différentes de mort, comme la recherche du sensationnel ou de l'éclat » (Lichtenstein et al. 1978 p. 552). Slovic et al. (1979) indiquent que la disponibilité est affectée par plusieurs facteurs sans lien avec la fréquence estimée du risque. En effet, Kermisch (2010 p. 19) explique qu'il s'agit pour l'individu **d'estimer la facilité de se remémorer l'événement, sans « pour autant effectuer réellement l'opération de remémoration »**. Ce biais ne peut alors être évoqué sans tenir compte des trois caractéristiques qui peuvent l'influencer soit la familiarité de l'évènement, sa saillance, et l'occurrence récente d'évènement (op. cit.). En ce sens Lichtenstein et al. (1978) et Slovic et al. (2004) citent plusieurs exemples dans lesquels les fréquences des risques sont surestimées par une surexposition médiatique (tels que la mort par homicide ou les accidents) alors que ceux qui sont sous médiatisés ont une fréquence sous-estimées (tels que les morts dus au diabète ou aux infarctus). Ils concluent que **plus les risques sont sensationnels, plus ils sont médiatisés et plus leurs fréquences sont relativement surestimées** (op. cit.) Cette conclusion prend tout son sens dans les propos de Slovic et al. (1980 p. 9) qui ont étudié les raisons possibles évoquées lorsqu'une voiture se trouve dans l'incapacité de démarrer en statuant que « **ce qui est en dehors de la vue est effectivement en dehors de l'esprit** ».

Notons que Sjöberg et al. (2004) émet une réserve sur les constats de ces chercheurs. En effet, il souligne que ces recherches ont été effectuées sur la base de risques dont les conséquences sont médiatisées, alors que d'autres conséquences, telles que celle d'un accident nucléaire, peu nombreuses et ainsi moins évoquées auprès du grand public à la période de ces études[47], sont également surestimées malgré une « disponibilité » faible. Sjöberg et al. (2004), à l'appui de ce constat, renforce l'intérêt pour la théorie culturelle du risque en s'interrogeant sur les relations fortes entre le risque perçu et l'ampleur de la couverture médiatique.

L'heuristique d'affect (Finucane et al .2000) établit la mise en perspective du bénéfice attendu pour l'évaluation du risque (cf. « 3.2.2 Concepts de l'étude des risques », section « Le risque acceptable » p. 114). Nous rappelons que cet heuristique guide l'acceptabilité du risque en définissant qu'un individu juge faible le risque et élevés les avantages s'il a un **sentiment favorable pour l'activité risquée**. Cadet et Kouabénan (2005 p. 22) précisent

[47] Avant 1979 et l'accident de la centrale de Three Mile Island, deux autres accidents de catégorie 5 (entraînant un risque hors du site) sur l'échelle INES sont survenus (fr.wikipedia.org/wiki/Liste_d'accidents_nucléaires, consulté le 20 avril 2018)

ainsi que « l'évaluation cesse ainsi d'être une activité purement "raisonnée" d'où les sentiments et les affects sont exclus ; il est désormais tenu pour acquis que des facteurs de type affectif ou de personnalité sont opérants, à côté d'informations réputées purement cognitives ». Ainsi, fournir davantage d'informations aux évaluateurs modifie leur appréhension du risque et réciproquement (Finucane et al. 2000). Ces résultats contribuent à l'hypothèse formulée par Slovic et al. (2004), considérant que les biais de disponibilité sont liés à l'affect, attendu que celui-ci peut accroitre la présence et la prégnance d'informations.

Particulièrement à nos travaux dans le champ de la SSI, et en nous attachant au concept de disponibilité, à savoir, pour l'évaluateur, de disposer mentalement de situations comparables, nous notons qu'il est peu aisé de définir l'influence de la médiatisation des risques SI. En effet, rappelons que la SSI est un sujet sensible pour les organisations (Kotulic et Clark 2004) et n'a alors pas vocation à être rendu publique, au contraire. Ainsi, outre la vague d'attaque de 2016 ciblant les États-Unis[48] et celle, mondiale, de 2017 liées aux ransomwares[49], les dysfonctionnements SI des entreprises sont, selon nous, peu communiqués.

Liés par plusieurs auteurs au concept de biais de disponibilité, il convient alors d'évoquer le biais de représentativité et d''ancrage-ajustement (Cadet et Kouabénan 2005 ; Hermand et Chauvin 2008 ; Kermisch 2010).

Représentativité

La représentativité consiste à rattacher la situation à évaluer à une classe déjà connue de situations similaires, classe ou schéma (Amalberti 1996), selon ses caractéristiques types (Hermand et Chauvin 2008). Elle est utilisée lorsqu'un évaluateur doit déterminer la probabilité que l'évènement A soit comparable à un évènement B connu (Kermisch 2010). Le terme représentativité signifie alors la reconnaissance d'une situation, basée sur ses connaissances, croyances, expériences et de l'environnement, à des situations antérieures qui paraissent similaires (Sjöberg 2000). Ce processus provoque alors une distorsion qui « occulte complétement d'autres sources d'information, ou les règles élémentaire de traitement de celle-ci » (Kermisch 2010 p. 21). Ce biais a pour conséquence de masquer la faible ressemblance d'une situation inadaptée à l'évènement qui doit être évalué (Amalberti

[48] Mirai, octobre 2016(fr.wikipedia.org/wiki/Mirai_(logiciel_malveillant) consulté le 20 avril 2018)

[49] Wannacry, mai 2017 (fr.wikipedia.org/wiki/WannaCry consulté le 20 avril 2018) et Notpetya, juin 2017 (fr.wikipedia.org/wiki/Cyberattaque_NotPetya consulté le 20 avril 2018)

1996) pouvant conduite à des erreurs de jugement (Slovic et al. 1982 p. 85). Ainsi, l'évaluation de la probabilité de survenance du risque, ou autrement nommée sa fréquence, relève davantage de la capacité de l'évaluateur à identifier une situation similaire plutôt qu'à identifier une fréquence réelle de classe et schéma auxquels le risque est comparé.

En ce sens, Kermisch (2010) soulignent que les évaluateurs ne sont pas sensibles à la taille de l'échantillon de données, soit le nombre de situations comparables. Précisément, selon elle, la preuve a été faite que « si l'information émane de deux échantillons de taille inégale, l'individu interrogé leur accorde le même intérêt au lieu de privilégier l'échantillon le plus grand ». Ce biais accentuerait alors une possible erreur d'estimation car l'évaluateur s'attacherait à identifier une situation « comparable » qui peut être moins représentative que plusieurs autres.

Une fois la situation de comparaison remémorée, l'évaluateur considère ensuite ce cas précédent pour décider et l'ajuste en regard de ses enjeux et de la situation, il s'agit de l'ancrage-ajustement.

Ancrage-ajustement

L'ancrage-ajustement consiste à réaliser l'évaluation en prenant comme référence certaines valeurs antérieures de risque comme point de départ (ancrage) en y apportant quelques modifications (ajustement) pour tenir compte du contexte présent (Cadet et Kouabénan 2005 ; Hermand et Chauvin 2008). Selon Kermisch (2010 p. 23) plusieurs chercheurs ont expliqué le rôle du point de référence comme « première approximation du jugement » lors de la « quantification de valeurs incertaines ». Ensuite, l'évaluateur procède à des ajustements en intégrant des informations supplémentaires dont la valeur accordée est moindre par rapport à la valeur de référence.

En ce sens, Slovic et al. (1984 p. 184) indiquent que si un individu a établi un « avis initial fort » d'un risque, alors ses croyances pourront « structurer la façon avec laquelle la preuve ultérieure est interprétée ». En d'autres termes, les nouvelles informations dont l'évaluateur disposera pour traiter le risque, si elles ne sont pas compatibles avec sa croyance initiale, seront considérées **comme moins prégnantes, voire fausses**.

Pour Cadet et Kouabénan (2005 p. 10), si l'analyse a pour finalité un diagnostic permettant la décision, elle ne doit pas seulement tenir compte d'éléments convergents, « c'est-à-dire qui se trouvent être en accord pour indiquer l'existence d'un état sous-jacent » mais aussi de

considérer « des informations qui vont à l'encontre de cette opinion initiale ». Si cette procédure permet d'éviter le biais d'ajustement, elle nécessite de faire cohabiter des indices qui peuvent être contradictoires, rendant la définition et l'évaluation des risques « singulièrement compliquées » (Cadet et Kouabénan 2005 p. 10). Ce procédé va à l'encontre des commentaires de Slovic et al. (1979) qui évoquent la « persistance des opinions » pour laquelle la présence de preuves contradictoires ne modifie que très faiblement le jugement initial. Pour ces mêmes auteurs, cela peut s'expliquer parce que les informations reçues et traitées après le jugement initial sont **justement cadrées** par ce dernier. Pour Kermisch (2010 p. 23) « ce biais n'est pas sans conséquence au niveau de la gestion des risques, puisqu'il montre que la présence de preuves ne suffit pas à éliminer les désaccords en matière d'estimation des risques ».

Ce constat renforce l'idée que les évaluateurs semblent peu enclins à modifier leur opinion de départ, conduisant à deux autres biais, l'effet de cadrage et l'excès de confiance.

Effet de cadrage

S'agissant de l'ancrage-ajustement, l'ancrage des schémas est souvent soumis aux effets de contexte, autrement appelé « framing effect » (Tversky et Kahneman 1981). Amalberti (1996 p. 86) rappelle que les schémas « sont des structures de données destinées à représenter des situations génériques ». Ces schémas sont caractérisés par l'atteinte d'un but pour lequel est effectué un processus de recherche d'information et de choix d'actions. Selon Cadet et Kouabénan (2005 p. 23) les schémas permettent « de mettre en œuvre simultanément trois types d'activités de traitement : identifier une situation, appliquer les règles adéquates, créer de nouvelles règles ». Ces schémas conditionnent alors la façon dont les individus sensibles à la forme de la représentation des informations (Kermisch 2010). Slovic et al. (1984) soulignent l'importance de la présentation et de la formulation du problème qui oriente manifestement le choix de l'évaluateur (Slovic et al. 1984) En effet, de nombreux exemples « d'effet de cadrage » ont été démontrés par Tversky et Kahneman (1981) et Slovic (2016) et illustrés dans la figure 16. Les évaluateurs prennent en compte d'autres considérations de traitement des informations comme des effets de compatibilité, d'ancrage du schéma retenu et des heuristiques de choix (Slovic et al .1984). Nous pouvons illustrer ces constats par une étude présentée par Slovic et al. (1984) dans laquelle deux populations sont exposées à deux choix identiques mais présentés différemment. Dans cette étude, il a été demandé à des individus d'imaginer qu'ils avaient le cancer du poumon et de choisir entre deux thérapies,

soit la chirurgie, soit la radiothérapie. Pour certains des interviewés, les résultats de probabilité ont été présentés en termes de survie alors que d'autres se sont vus présenter les mêmes probabilités en termes de mortalité. Les individus choisissent la thérapie exprimée en termes de survie et écartent la thérapie systématiquement exprimée en termes de mortalité, quel que soit le type de thérapie considérée dans l'analyse et l'acceptation du risque.

Un autre biais, l'excès de confiance est directement lié à l'ancrage-ajustement et à l'effet de cadrage puisqu'il conduit à écarter des solutions alternatives.

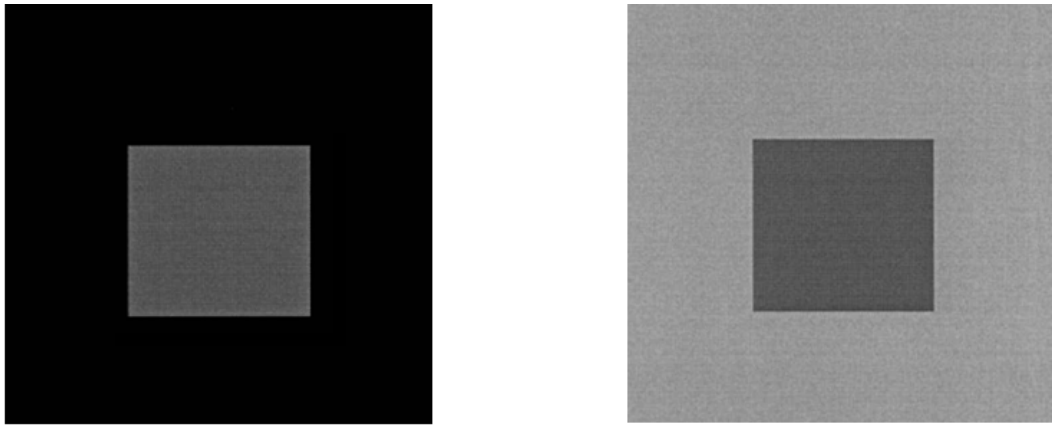


Figure 16 : Dépendance de référence dans la perception de luminosité[50]

(Kahneman 2003 p. 1455)

Excès de confiance

Pour Slovic et al. (1979 p. 16), un « aspect particulièrement pernicieux des heuristiques est que les individus sont généralement confiants sur les jugements » qui en résultent. Il s'agit d'un autre facteur des distorsions qui entraine des répercussions dans les estimations d'évènements redoutés, « **voire à nier leur existence** » (Cadet et Kouabénan 2005 ; Kermisch 2010). Ainsi, Slovic et al. (1980) constatent qu'une fois les évènements classés en fonction de leur niveau de mortalité potentielle, les individus estiment leurs réponses correctes, sans considérer le caractère incomplet des informations traitées, témoignant alors

[50] Kahneman 2003 p. 1455 : explique l'illustration de « la dépendance de référence dans la vision » Si les deux carrés intérieurs ont strictement la même couleur, leur brillance n'apparait pas égale. La démonstration consiste en ce que la luminosité d'une zone n'est pas une fonction à un seul paramètre de l'énergie lumineuse. Il est nécessaire de tenir compte de luminosité perçue avec un paramètre pour de référence, qui est influencé la stimulation actuelle et antérieure.

une confiance excessive (Kermisch 2010). Cadet et Kouabénan (2005) illustre ce biais en indiquant qu'un individu **ayant réussi à traiter des situations risquées complexes et comparables** (telles que des situations professionnelles) **sera enclin à minimiser la présence de risque** et l'ampleur des conséquences. Ainsi l'opérateur ou le pilote chevronné place-t-il dans les qualités de son système technique ou dans ses propres capacités une confiance qui peut s'avérer excessive en cas de difficultés (Amalberti 1996). Slovic et al. (1980) et Kermisch (2010) prolongent ce constat en mentionnant que les experts d'un domaine sous-estiment les risques par leur incapacité à anticiper 1) l'impact des erreurs humaines sur les systèmes technologiques, 2) le comportement humain en regard de mesure de sécurité, 3) à observer un système technologique dans son ensemble et dans son environnement, et 4) les erreurs de défaillances multiples issues de mêmes causes.

Selon Kermisch (2010) l'excès de confiance rejoint le biais « d'optimisme irréaliste ». Sjöberg et al. (2004 p. 10) précise ce biais comme « un optimisme général à propos du résultat d'un événement ». Ainsi, « dans un groupe, la grande majorité des individus perçoivent leurs chances que survienne un événement négatif comme inférieures à la moyenne, alors ceci n'est clairement pas juste optimiste mais aussi peu réaliste » (op. cit.). Kermisch (2010) illustre l'optimisme irréaliste par l'attitude d'individus exposés à un risque manifeste (tel que vivre dans une zone inondable) tout en croyant ne courir aucun risque. Ce constat renvoie à la supposition que les individus pensent contrôler le risque, sans doute développée par la volonté de **réduire l'anxiété inhérente** en écartant la cause du risque (Kermisch 2010). Ainsi, pour Sjöberg et al. (2004 p. 10) « les **individus ont un sens fort mais injustifié d'immunité subjective ».** Un individu peut être insensible à un risque, dont il peut juger la probabilité et l'impact grave, car il **s'estime faiblement exposé** par rapport à d'autres individus. Pour Peretti-Watel (2000), en prolongement de ce constat, évoque un écart de perception pour l'individu lui-même et pour les autres, suggérant que l'individu est moins exposé notamment parce qu'il pense pouvoir justement contrôler le risque. Ces remarques sont en accord avec les faiblesses des dispositifs de sécurité de l'information évoqué par Taylor (2015 p. 177), construits sur « des méthodes actuelles d'évaluation de sécurité de l'information biaisées parce que les décisions quant à la sécurité de l'information sont souvent basées sur les heuristiques et des perceptions optimistes ».

L'insensibilité aux probabilités

Un autre biais dans l'évaluation d'un risque, défini par son impact et sa probabilité, relève de la considération de cette dernière par les individus. Plusieurs auteurs ont souligné l'importance de la valeur subjective (Cadet et Kouabénan 2005 ; Slovic et al. 2004) sur laquelle l'évaluation et le traitement du risque s'appui. « Concrètement, cela signifie que les **estimations ne peuvent pas être linéaires** chaque fois que la valeur éprouvée d'une unité dépend des autres caractéristiques de la situation ou de la situation dans son ensemble » (Cadet et Kouabénan 2005). Pour Slovic et al. (1984 p. 200), les implications de la valeur subjective se situent dans les « signes » renvoyés par l'ampleur et la nature des conséquences d'un risque. Par exemple, un accident sera considéré comme sérieux, quelles que soient les conséquences, s'il remet en cause la probabilité ou les conséquences perçues de cette catégorie d'évènement (Slovic et al. 1984). À l'inverse, un accident dont les conséquences sont familières, issu d'un dysfonctionnement compréhensible et n'offrant **pas de véritable différence sur son potentiel catastrophique ni sa probabilité perçue, n'aura que peu ou pas d'impact sur les croyances et connaissances** de l'évaluateur. Selon ces principes, le concept d'accident comme signal peut éclairer la perception des risques nucléaires. En effet, ces risques sont perçus comme incompris et catastrophiques, engageant peu de vies humaines directes et dont le coût est majeur pour la société (Slovic et al. 1984). Selon nous, cet exemple illustre la rationalité inverse de la volonté de réduire autant que possible un risque dont la probabilité est faible. Une autre catégorie d'accident confirme la généralisation de ce concept. L'accident routier est compréhensible et familier, engage un nombre réduit de vies et il ne suscite pas de volonté marquée de réduction, ce qui interroge sur la fréquence (probabilité) considérée par les évaluateurs (cf. Tableau 6 : Résultats partiels des risques perçus et bénéfices perçus). En ce sens, Cadet et Kouabénan (2005 p. 28) soulignent « l'insensibilité relative à la perte de vies humaines dans les catastrophes de grande ampleur ou dans **les risques répétitifs** (risque routier par exemple) ». Pour ces auteurs la variabilité de la valeur subjective est également mise en évidence dans une autre étude. Les chercheurs se sont intéressés au risque de cancer lié au tabac. Ils ont démontré que si l'idée de dangerosité du tabac est vérifiée, « les cigarettes additionnelles sont évaluées comme de moins en moins nocives à mesure que croît la consommation journalière » (Cadet et Kouabénan 2005 p. 28). En ce sens, l**'exposition au risque est justement perçue comme diminuée dès lors que les évaluateurs estiment contrôler la situation** (Chauvin et Hermand 2006). Des résultats comparables sont également soulignés par plusieurs études de Slovic et ses collègues. Ainsi, Slovic et al. (1984)

ont montré que les individus privilégient pour le traitement du cancer le choix présenté sous la forme de survie marquant la prégnance des valeurs subjectives aux dépends des probabilités (cf. « Effet de cadrage). Ensuite Slovic et al. (2004) ont conduit une étude où la préférence du répondant est de sauver 98% de 150 vies grâce à des équipements spéciaux embarqués dans les avions, alors que ces mêmes équipements pourraient sauver 150 personnes. Ces mêmes auteurs expliquent que le taux élevé de vies potentiellement sauvées (98%) prévaut sur le nombre.

En complément de l'exposé des trois paradigmes d'étude et de la théorie culturelle des risques, nous avons présenté les influences possibles que pouvaient activer les évaluateurs. Ainsi, l'objectif de ces sections a été de comprendre, dans un champ académique différent de la SSI, soit la psychologie, comment les risques peuvent être pris en considération et évalués par les individus, pour accepter ou réduire les conséquences potentielles ou encore son exposition potentielle. Cela permet d'avoir une vision précise des risques, de leurs influences et de leurs interactions sur la volonté d'un décideur de réduire le risque, soit d'adopter symboliquement la SSI. En effet, nous rappelons que la première étape pour la mise en œuvre de la SSI, selon Straub et Welke (1998) est justement d'analyser les risques.

Ainsi, la perception et l'analyse de risque au niveau individuel semble tout à fait pertinentes pour éclairer les éléments considérés et leurs influences dans la prise de décision symbolique la SSI. Particulièrement, nous avons noté plusieurs travaux académiques dont l'intérêt a été justement d'explorer l'articulation entre risques perçus et SSI.

3.2.7. Perception des risques et SSI

À notre connaissance, huit travaux académiques combinent perception des risques et SSI (Albrechtsen 2007 ; Albrechtsen et Hovden 2009 ; Loch et al. 1992 ; Straub et Welke 1998 ; Huang et al. 2010 ; McFadzean et al. 2007 ; Taylor 2006 ; Tsohou et al. 2006). De nombreuses recherches soulignent que la SSI nécessite la décision et l'implication de la direction générale (Eloff 1988 ; Knapp et al. 2006 ; Siponen 2000 ; Solms 1996 ; Soomro et al. 2016 ; Straub 1990). Les huit travaux que nous avons identifiés dans la littérature s'appuient sur ce constat et considère la SSI en regard des décisions pour les risques qui exposent l'organisation. Si l'objet de ces travaux est majoritairement de porter un éclairage nouveau sur la prise de décision quant à la SSI et en regard des risques SI, notons que tous ne s'appuient pas sur un cadre théorique de perception des risques.

Avant d'en dresser une synthèse, nous présentons ci-après ces travaux dans l'ordre chronologique de parution et les mettons en perspective de la littérature des trois paradigmes d'étude et de la théorie culturelle des risques.

Loch et al. (1992), Réalité des menaces d'aujourd'hui, compréhension d'hier

Après avoir décliné les **menaces** issues de la littérature et qui exposent les SI, Loch et al. (1992) ont étudié comment elles étaient perçues par les top-managers. Ainsi, l'étude porte sur la **perception des menaces et non pas des risques**. Rappelons que le risque peut se définir par la combinaison d'une menace et une probabilité de perte (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Dhillon et Torkzadeh 2006), écartant alors le risque de l'étude de Loch et al. (1992). Précisément, les deux questions posées sont 1) « quelles sont les menaces pour les SI et les données » et 2) « lesquelles d'entre elles sont les plus sérieuses » (Loch et al. 1992 p. 175). Ainsi, ces auteurs ont élaboré un instrument de mesure afin de questionner les tops-managers pour qu'ils classent les 12 menaces de la plus importante à la moins significative. Si les résultats positionnent la menace environnementale, la destruction et la mauvaise saisie de données par les utilisateurs comme les plus redoutées, il nous apparait une incohérence pour le domaine « micro-informatique ». En effet, les réponses évoquent une crainte importante des menaces extérieures à l'organisation alors que près de la moitié relèvent d'acteurs internes à l'organisation (les 5 premières menaces représentent 71,8% des réponses avec 11,7 % pour l'environnement et 60,1% pour la destruction et la mauvaise saisie de données, l'inadéquation des contrôles ou leur inefficacité). Ainsi, Loch et al. (1992 p. 185), à l'appui des travaux de Straub (1990), révèlent une « ironie » de la SSI. Selon eux, les répondants semblent conscients des menaces tout en « percevant le risque comme modérément bas » et en considérant l'entourage de l'organisation plus exposé au risque qu'eux-mêmes (op. cit.). Loch et al. (1992 p. 185) émettent l'hypothèse sur l'explication de ce dernier constat par la **« croyance plutôt naïve que de mauvaises choses arrivent seulement aux autres »**. Cette hypothèse est en accord avec les constats de Peretti-Watel (2000), qui évoque une perception plus faible pour l'individu lui-même que pour les autres, car il pense contrôler le risque et par conséquence y est moins exposé, suggérant que les autres n'ont pas le même niveau de maitrise.

Les résultats de cette étude suggèrent d'informer les top-managers 1) du potentiel pour des infractions de sécurité des SI, 2) qu'une faible préoccupation pour la sécurité peut indiquer

une sous-estimation des risques SI potentiels « inhérent à environnement fortement connecté » (Loch et al. 1992 p. 185). En synthèse, si nous sommes en accord avec la question posées par Loch et al. (1992) sur l'utilisation de nouvelles technologies en regard des risques qui les exposent, nous soulignons la confusion des concepts mobilisés dans leur étude, soit menace, qui écarte la notion de perte, et risque global.

Straub et Welke (1998), faire face aux risques, modèles de planification de sécurité pour les décisions de management

Sur la base du constat de SI insuffisamment protégés, notamment par l'absence d'investissement des top-managers pour la SSI, Straub et Welke (1998) établissent un modèle de gestion des risques SI. Ils adossent leur modèle aux travaux de Goodhue et Straub (1991), à la théorie de dissuasion générale (Straub 1990) et au modèle de prise de décision de Simon. Si pour Straub et Welke, le risque SI est élevé, ils citent Loch et al. (1992 p. 183) pour qui « beaucoup d'organisations sont sous-sécurisées, beaucoup de managers continuent à ignorer la question et à être "naïfs" dans leurs réponses au défi posé par cette menace croissante ». Une des raisons principales à ce constat est, selon Straub et Welke, que le risque SI a été ignoré, « durant des décennies » même pour les top-managers spécialisés en IT et il est difficile de changer une perception dans cette dynamique (désigné par les auteurs comme « back-burner issue », Straub et Welke, 1998 p. 442). Ainsi, ils s'interrogent sur le gap entre menaces sur les SI, répandues, avérées et appuyées, et le manque de préparation des tops-managers. Ils proposent alors de s'intéresser à la perception managériale des risques et soutiennent qu'elle est **fonction 1) des risques inhérents à l'industrie, 2) des mesures de sécurité définies pour contrôler ces risques et 3) des facteurs individuels comme les expériences sur la SSI**, tels que présentés dans la figure 17. Ils suggèrent un modèle permettant la mise en œuvre de mesures de sécurité qui tienne compte d'une planification systématique des étapes d'analyse des risques, d'apprentissage de la sécurité et d'étude de la réponse possible aux risques.

Soulignons que l'approche méthodologique de Straub et Welke définit le risque comme une menace pouvant provoquer des conséquences sur l'organisation et non pas sur les seuls SI (soit une approche de protection globale telle que développée notamment par Dhillon et Backhouse, 2001 ou Herath et Rao, 2009a, comparée à une approche seulement technologique de la SSI). En effet, ils développent le concept de « system risk », dans lequel « les informations de la société et/ou des systèmes d'information ne sont pas suffisamment

protégés contre certaines sortes de dégâts ou de pertes », étendant la perte non pas seulement au SI mais à ses conséquences « métier » (Straub et Welke 1998 p. 442-443). Ainsi, dans leur étude, la perception des risques est centrée sur les risques SI dont les interviewés ont connaissance ou qu'ils doivent « imaginer » (cf. Straub et Welke 1998, Scénario A et B, p. 466).

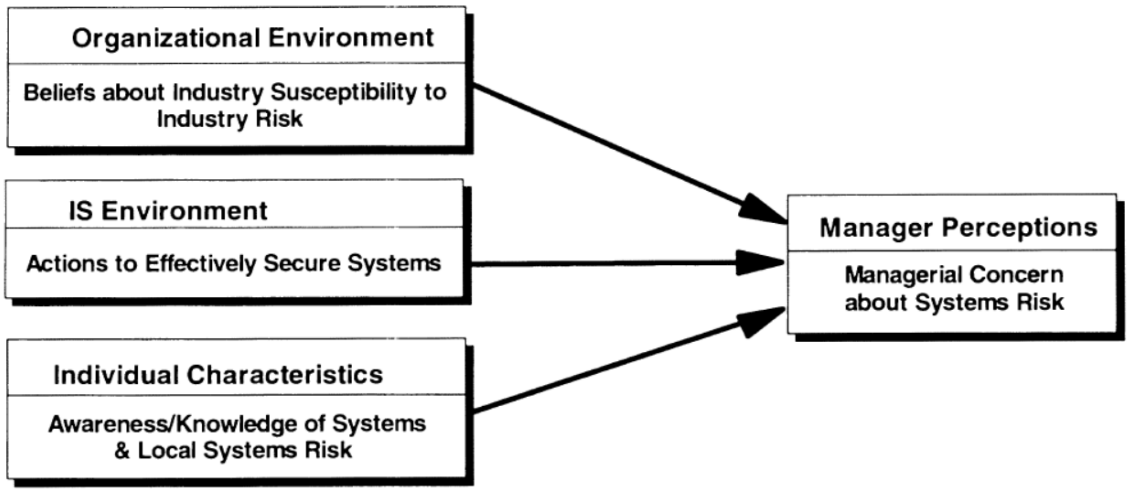


Figure 17 : Modèle des perceptions managériales des risques SI
(adapté de Goodhue et Straub 1991 par Straub et Welke 1998)

Ils s'interrogent sur la façon dont la conscience des top-managers doit être « intensifiée », en mettant en perspective un modèle dont la validité repose les « trois composants sous-jacents de risque affectant leur perception globale » (Straub et Welke 1998 p. 444). Le premier composant permet précisément d'étudier la façon dont les top-managers « développent leurs croyances sur les risques » en regard des organisations comparables, bien que Straub et Welke (1998 p. 444) précisent que ce sujet est « au-delà du périmètre de la recherche actuelle parce qu'il implique la lecture relativement directe et / ou le partage de connaissance du risque parmi des groupes d'industrie ». Le deuxième et le troisième composants permettent d'appréhender la façon dont les top-managers sont informés des incidents sur leurs SI et des mesures mise en œuvre et potentielles. Si les deux derniers composants nous semblent pertinents en tant qu'influence dans le processus de planification de la SSI, le premier nous apparait aussi prégnant et en accord avec les paradigmes de perception des risques. Rappelons que la perception des risques s'inscrit justement « dans le cadre de la théorie de décision comportementale » (Slovic et al. 1984 p. 183), et qu'elle vise à

déterminer les pertes potentielles et définir la probabilité de ces pertes afin de déterminer les décisions à prendre quant au risque (Yates et Stone 1992). Dans nos travaux, nous proposons ainsi de repositionner la perception des risques SI en tant qu'influence sur la décision, selon les trois composants de Straub et Welke(1998).

En conclusion de leur étude, Straub et Welke soulignent la connaissance partielle des top-managers sur les mesures de sécurité possibles, limitant alors leur intérêt pour les risques SI. En regard de la littérature sur la perception des risques, ce commentaire n'est pas significatif et s'inscrit plutôt selon l'articulation expert / profane (Yates et Stone 1992). En effet, ce commentaire relève précisément de l'approche technologique des risques et des mesures de sécurité à mettre en œuvre, sur lesquels les top-managers devraient disposer de connaissances au sens de Straub et Welke. L'approche organisationnelle de la SSI permet justement d'analyser les risques avec les top-managers et selon une vision métier (Choobineh et Dhillon 2007 ; Dhillon et Backhouse 2001) pour ensuite décliner les mesures de sécurité et protéger les SI, en s'appuyant sur des expertises techniques.

Taylor (2006), perception managériale des risques involontaires sur la sécurité de l'information

Taylor (2006) s'appuie sur le concept de la « cécité des exécutifs » développée par Slovic et al. (1987) pour explorer l'approche réactive aux menaces pesant sur les SI par les top-managers. Il affirme que ces derniers « ont tendance à avoir une perception incorrecte des événements en ignorant les probabilités et utilisant à la place des mécanismes heuristiques pour mesurer l'incertitude ou éviter de les traiter » (Taylor 2006 p. 1585) en accord avec Cadet et Kouabénan (2005) et Slovic et al. (2004) qui indique une valeur subjective comme référence à l'évaluation[51]. L'étude de Taylor vise à comprendre la perception globale les managers des risques SI et des actions des salariés pouvant involontairement exposer leur organisation. S'il soutient mobiliser la théorie de perception des risques de Slovic et al. (1986), il détaille peu la méthode employée et l'articulation entre les risques abordés dans la phase empirique et les concepts de Slovic.

Ainsi, Taylor a analysé une organisation financière pour conclure la validité de ses trois propositions, à savoir que le management perçoit 1) un haut niveau de sécurité de ses SI, 2)

[51] Afin d'éclairer notre propos, rappelons l'exemple de Slovic et al. (1984) pour qui un évaluateur considère un accident comme sérieux qu'à la condition où ses probabilités de survenance sont remises en cause.

une forte adhésion aux politiques de sécurité établies, 3) l'absence de risque liée à une action involontaires des collaborateurs. Plus globalement, la direction générale de l'organisation étudiée perçoit « leur niveau de sécurité de l'information comme élevé » et « les cadres ont unanimement reconnu que la sécurité était au-dessus de la moyenne et qu'ils mettaient tout en œuvre pour protéger les informations de l'organisation » (Taylor 2006 p. 1593).

Nous notons dans la discussion de Taylor trois points majeurs qui sont en accord avec la littérature SSI. Premièrement, la sur-confiance accordée par la direction générale aux résultats d'audit tiers à conduit à une fausse impression de sécurité. Basé sur les seuls aspects technologiques de la sécurité, ces audits n'ont pas révélé les risques externes et internes auxquelles l'organisation est exposée. Deuxièmement, la DSI de l'organisation s'est limitée à ces rapports qui la positionnent favorablement vis-à-vis de la direction générale, sans l'encourager à analyser le champ global de la sécurité du SI et particulièrement les aspects humains. Ce constat est en accord avec plusieurs auteurs qui soulignent le périmètre technologique de la SSI, dont la filiation à l'IT la limite aux seuls aspects techniques (Doherty et Fulford 2005 ; Posthumus et Solms 2004). En ce sens, Taylor (2006 p. 1593) s'appuie sur les travaux de Whitman (2003) pour rappeler que « … nous négligeons souvent la solution humaine et optons au lieu de cela pour des solutions technologiques, alors que le facteur humain doit être d'abord adressé, avec une aide technologique pour assurer l'exécution de comportements humains souhaités ». Troisièmement, sur le concept de la seule réponse aux menaces perçues de Fischhoff et al. (1978) et Slovic et al. (1980), les managers ne perçoivent pas comme risqué les actions involontaires de leurs subordonnés, pouvant mettre en défaut la sécurité du SI, rejoignant le constat de Barlette et Fomin 2010 (p. 128) qui précisent que la priorité est donnée aux menaces externes tels les hackers ou les virus.

Sur la base de ses résultats, Taylor (2006 p. 1594) souligne la nécessité de positionner l'humain au cœur du dispositif de SSI « en commençant par le sommet de la hiérarchie organisationnelle » **pour modifier leur perception des risques et influencer directement la façon dont les risques sont abordés**. Ainsi, si cette étude met en exergue ce besoin, elle est plutôt silencieuse sur les risques perçus et la façon dont ils sont interprétés pour la protection des SI de l'organisation.

Tsohou et al. (2006), formulation de stratégies de gestion des risques SI par la théorie culturelle

Tsohou et al. (2006) ont appréhendé le potentiel de la théorie culturelle sur la perception de et la gestion des risques SI. Nous rappelons que la théorie culturelle du risque complète la perception des risques du paradigme psychométrique par la prise en compte des incertitudes selon les styles de pensée qui régissent l'action sociale des individus (cf. « 3.2.5 Paradigme psychométrique », section « La théorie culturelle du risque » p. 140). Pour Tsohou et al. (2006), la théorie culturelle soutient la prévisibilité de la perception de risque dans les groupes et les structures sociales, selon les visions individuelles du monde. Sur cette acception, leur étude théorique vise à observer les risques perçus par les top-managers et les réponses qui y sont apportées. Tsohou et al. (2006 p. 201) précisent que la mitigation des risques est basée sur la norme ISO 27001 (2005) au travers des phases « de conception, d'implémentation et de surveillance »[52]. Basée sur ces étapes de gestions des risques et sur les travaux de Douglas et Wildavsky (1983), Tsohou et al. (2006) élaborent un phasage pour les normes des structures sociales d'organisation de la SSI. Ces travaux offrent une vision prospective des méthodes de risques privilégiées, des risques redoutés et des types de mesures de sécurité.

Si les travaux de Tsohou et al. (2006) sont exploratoires et théoriques, le lien avec les risques SI semblent peu développés. En effet, ils mettent en perspective des choix de méthodes de gestion des risques en regard des types de biais culturels. Par exemple, ils supposent que les individus du type « égalitariste » préfèrerons utiliser des méthodes qui « encouragent la participations des parties prenantes » alors que les « individualistes » choisiront des méthodes basées sur les couts et les bénéfices » Tsohou et al. (2006 p. 208). Ensuite, ils énoncent le type de risques redoutés, en accord avec les valeurs sociales attribuées à chaque type de profil par Douglas et Wildavsky (1983). Notons, qu'il s'agit davantage de la façon dont sont considérées les menaces redoutées que des risques pour le SI lui-même. En effet, rappelons que le concept de risque SI, reconnu dans la littérature SSI, revêt à la fois une menace et une probabilité de perte (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Kayworth et Whitten 2010 ; Loch et al. 1992 ; Straub et Welke 1998 ; Dhillon et Torkzadeh 2006). Par exemple, selon Tsohou et al. (2006 p. 213), les menaces sont observées par les « égalitaristes » sous « l'angle de l'équité » et en cherchant

[52] Soulignons que la norme ISO 27001 (2005) et son évolution (2013) ne définissent pas l'approche de gestion des risques mais qu'il s'agit d'un standard pour « fournir un modèle d'établissement, de mise en œuvre, de fonctionnement, de surveillance, de réexamen, de mise à jour et d'amélioration d'un SMSI » (Système de Management de la Sécurité de l'Information (SMSI, ISO 27001 2005 p. V)

« l'exhaustivité des informations pour réaliser leur propre analyse ». Enfin, les mesures de sécurité définies ne sont pas des contremesures aux risques mais des comportements attendus vis-à-vis de ces mesures. Par exemple, les « individualistes » sont attendus pour être réfractaires aux mesures et aux règles de sécurité qui les contraindraient. Ainsi, pour un type de biais culturels, Tsohou et al. précisent la façon d'aborder les risques (par type de méthode d'analyse) et les réactions face aux mesures de sécurité. Cela implique que les individus qui mobiliseraient la méthode d'analyse sont du même biais culturel que ceux qui appliqueront les mesures de sécurité. La littérature SSI précise justement qu'il ne s'agit pas des mêmes acteurs dans l'organisation pour la gestion des risques, les top-managers analysent les risques et définissent des mesures de sécurité (Goodhue et Straub 1991 ; Hu et al. 2007 ; Solms et Solms 2006a), alors que les utilisateurs sont appelés à les appliquer et à les respecter (Albrechtsen et Hovden 2009 ; Siponen et Vance 2010 ; Warkentin et Willison 2009). Si Tsohou et al. (2006 p. 207) soutiennent qu'un contexte donné et mutuel peut conduire les individus à « se conformer à des biais culturels différents », pouvant conduire à une acceptabilité partagée des risques (Fischoff et al. 1981 ; Slovic et al. 1987), Dake (1991) et Rippl (2002) ne partagent pas ce **constat et soulignent l'indépendance du contexte social** sur la conformité à un biais culturel.

Si nous pointons l'absence de considération pour le risque SI, nous soulignons l'intérêt de ces travaux qui mettent en perspective la perception des risques selon les biais culturels et influences sur la méthode d'analyse puis de traitement des risques. En ce sens, Tsohou et al. (2006 p. 214) appellent à confronter leurs apports théoriques dans une étude empirique et à observer ces problématiques « dans la gestion globale du management de la sécurité de l'information ».

Albrechtsen (2007), l'avis des utilisateurs sur la sécurité de l'information

Sur la base des travaux de Slovic (2000), Albrechtsen (2007) élabore deux constats. Le premier traite de la différence de perception des risques SI entre top-managers et utilisateurs « finaux ». Ces derniers pourraient **ne pas avoir la vision globale des activités** de l'organisation et ainsi **ne pas percevoir la nature et l'ampleur des risques**, accessibles au top-managers (Albrechtsen 2007). Le deuxième constat relève de la nécessité d'analyser et de communiquer les risques au sein de l'organisation, indépendamment des niveaux hiérarchiques. Il soutient que les désaccords sur les risques, entre experts et profanes d'une même organisation, peuvent être gommés par « une interaction bilatérale d'échange

d'informations, de discussion et d'approfondissement des alternatives » (Slovic 2000 p. 191). L'objet des travaux d'Albrechtsen est d'étudier le comportement individuel pour la sécurité de l'information. En effet, le point de vue d'un utilisateur sur la sécurité de l'information est influencé par plusieurs facteurs **organisationnels, technologiques et individuels** inter-reliés tels que les normes sociales et les interactions avec les autres collaborateurs, qui influencent la compréhension individuelle de la sécurité de l'information, les caractéristiques idiosyncratiques comme la motivation, la connaissance, les valeurs et le comportement (Dhillon et Backhouse 2000 ; Sjöberg 2002 ; Willison et Backhouse 2006) et la façon dont ils perçoivent le risque (Albrechtsen 2007 p. 277). Il rappelle que plusieurs facteurs, issus des travaux de Slovic (2000) tels que la non observabilité, l'absence de connaissance, la nouveauté ou l'incontrôlabilité des risques sont des caractéristiques majeures pour la perception des risque et qu'ils peuvent expliquer l'indifférence des utilisateurs pour la SSI (Albrechtsen 2007). Également, s'il précise que le « **le risque est subjectivement décidé** par les individus qui peuvent être influencés par un large éventail de facteurs psychologiques, sociaux, institutionnels et culturels » (Albrechtsen 2007 p. 277), il précise que **l'acceptation du risque relève aussi des avantages de la situation risquée et des coûts associés aux mesures de sécurité**. Ensuite, citant Wilde (1982), Albrechtsen indique quatre façon de traiter le risque perçu, soit 1) diminuer le bénéfice attendu par le comportement risqué, 2) diminuer le coût attendu d'un comportement prudent, 3) augmenter le bénéfice attendu du comportement prudent et, 4) augmenter le coût attendu du comportement risqué. Ainsi, selon cet auteur, le comportement des individus quant à la SSI ne peut s'observer qu'en améliorant la connaissance des influences de la perception et l'acceptation du risque, en considérant le caractère familier et contrôlable du risque (Albrechtsen 2007). En effet, les travaux de Wilde (1982) mettent en évidence le « **compromis individuel de sécurité sur la perception de risque de l'individu et ses critères d'acceptation de risque**, c'est-à-dire qu'ils ajustent leur comportement pour équilibrer le risque perçu et acceptable individuel » (Albrechtsen 2007 p. 486).

Son étude a été réalisée selon une méthode qualitative qui a conduit Albrechtsen à interviewer dix-huit utilisateurs dans un centre de service IT et dans un département de conseil d'une banque. Il en émerge trois principaux résultats que sont l'avis des utilisateurs sur leur rôle et responsabilité pour la SSI, les efforts perçus pour l'application des mesures de sécurité et l'évaluation de ces comportements sur le risque potentiel. Les deux premiers résultats traitent de l'application de mesures et sont alors hors du champ de notre étude. Le troisième résultat nous intéresse davantage car il met en évidence un manque

d'investissement des utilisateurs pour la SSI à cause d'une faible perception des risques. En effet, Albrechtsen précise que la connaissance des référentiels sécurité et les campagnes de sensibilisation se révèlent peu efficace pour informer les individus. Ces communications « top-down » visent à susciter les bons comportements sans évoquer leur finalité, répondre au risque SI (Albrechtsen 2007 p. 286). Ils ne répondent pas au besoin de connaissance des « frontières visibles du risque inacceptable » et interrogent globalement sur la familiarité du risque et ses conséquences connues, en accord avec le principe même du risque (Slovic et al. 1984) décliné au risque SI (Straub et Welke 1998). Ainsi ces faiblesses se traduisent par l'inadéquation des comportements pour la SSI qu'Albrechtsen (2007 p.280) relève :

- les répondants ne sont pas familiers avec les menaces possibles,
- les répondants ne sont pas au courant des conséquences possibles,
- chaque répondant effectue très peu d'actions pour la SSI,
- les répondants ne voient pas de problème potentiel quant à leur pratique sur le SI.

En synthèse de l'étude d'Albrechtsen (2007) nous retenons l'importance de la **connaissance des risques SI pour y répondre de façon adaptée**. En ce sens, Albrechtsen (2007 p. 277) souligne la préférence des utilisateurs à se concentrer sur le cœur de leur fonction plutôt que sur la prévention du risque SI selon une stratégie de *satisficing* telle que développée par March et Simon (1958). En effet, lors d'une journée d'activité durant laquelle les sollicitations sont multiples, les individus sont enclins à choisir l'option « satisfaisante » plutôt que de réaliser une évaluation des autres options, couteuse en temps et ressources, plaçant à un second plan les pratiques de sécurité. Plus particulièrement, nous pouvons souligner la convergence de ces commentaires avec l'appréhension des risques développée dans le champ psychologique de la littérature. Si Kermisch (2010 p. 23) indique la prégnance de la première approximation du jugement en présence de valeurs incertaines (alternatives), Slovic et al. (1984 p. 184) rappellent l'ancrage de ce choix qui ne pourrait être que renforcé, quelles que soient les preuves qui apparaitrait après la décision.

McFadzean et al. (2007), perception des risques et impact de l'IT existante sur la stratégie de sécurité de l'information au niveau exécutif

McFadzean et al. (2007) rappellent l'exposition forte des risques SI de l'organisation lorsque ses top-managers n'engagent pas de « diligence raisonnable » de la SSI. Ils pointent l'importance des rôles et responsabilités du niveau exécutif pour s'intéresser aux actions qu'ils prennent pour assurer la sécurité de leur SI. Particulièrement, ils mettent en

perspective les risques perçus et comment cette perception influence leurs propres actions quant à la SSI. En effet, selon McFadzean et al. (2007 p. 622), les top-managers disposent de la capacité d'évaluer les besoins de l'organisation de sécurité par une approche holistique, rejoignant les propos d'Albrechtsen (2007), d'une part. D'autre part les top-managers disposent « du pouvoir d'assurer que les nouveaux systèmes et procédures soient mis en œuvre de façon opportune ». Enfin, le rôle des top-managers pour la SSI est également lié à l'importance stratégique accordée au SI et d'une façon générale à tous les facteurs qui peuvent influencer le succès de l'organisation (cf. Figure 18).

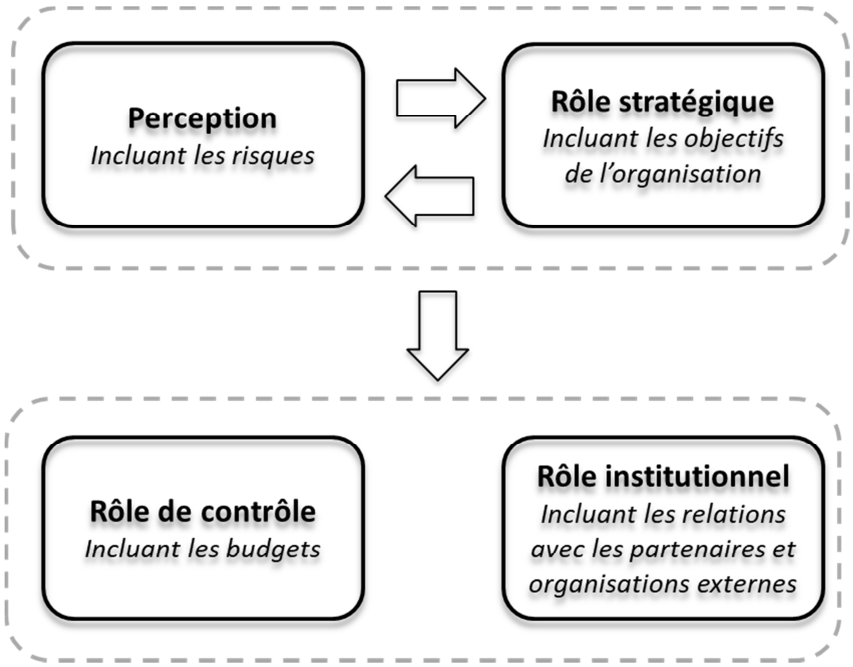


Figure 18 : Rôles des membres exécutifs

(adapté de Mcfadzean et al., 2007)

Quarante-trois top-managers de différentes entreprises ont été interviewés sur leur perception des risques SI, les pratiques de sécurité et l'environnement, telle que les exigences réglementaires ou les standards applicables, et enfin la façon dont la SSI affecte les processus d'affaires de l'organisation. Mcfadzean et al. concluent de l'analyse de ces entretiens que les **perceptions des exécutifs sur les risques ont un impact majeur sur la SSI**. Ils mettent en perspective ces risques des objectifs et de la stratégie de leur organisation, soulignant la possibilité de disposer d'un SI comme « une arme concurrentielle », rejoignant ainsi les propos de Sambamurthy et al. (2003), Kankanhalli et

al. (2003) et Vitale (1986), alors que d'autres n'en perçoivent pas l'importance ou voient leur SI comme une nécessité opérationnelle.

En synthèse, l'analyse de McFadzean et al. (2007) montre que l'engagement des dirigeants pour la SSI dépend de deux facteurs clés : **l'importance stratégique des SI** de leur organisation et **leur perception de risque**. Ces facteurs s'articulent alors avec quatre facteurs contextuels inhérents à la gouvernance d'entreprise : environnement, SSI, entreprise, législatif.

L'environnement inclus **les conditions externes** qui peuvent influencer la sécurité du SI, telles que des réglementations, des exigences de clients ou encore des actionnaires. En ce sens, Williams et al. (2009) dans le champ de la sécurité logistique constatent l'effet des demandes des clients sur l'amélioration des procédures de sécurité.

La SSI adresse particulièrement les **risques internes et externes** et le dispositif mis en œuvre pour y répondre. Ainsi, ce facteur contextuel comprend, selon Mcfadzean et al (2007), l'organisation des fonctions sécurité au sein de l'entreprise, les politiques et pratiques de sécurité, les compétences, les technologies et le contrôle de l'ensemble. Nous avons développé ces éléments et présenté le schéma global de la SSI, dans lequel s'articule, notamment, les éléments présentés par Mcfadzean et al. (cf. « Principaux thèmes de la recherche en SSI » p. 36)

L'organisation comprend essentiellement les **objectifs de l'organisation et sa stratégie**, sa culture, son niveau global de connaissance. Nous comprenons que c'est sur ce facteur que peut être observé l'importance accordée par les top-managers au rôle du SI, telle que présentée ci-avant. Ces aspects sont détaillés au chapitre « 2.4.1 Gouvernance » (p. 41) dans lequel est souligné le rôle du SI pour la création de valeur de l'organisation. À l'inverse, nous considérons effectivement qu'un SI dont l'intérêt pour l'organisation n'est pas établi sera sans doute assorti d'un faible investissement pour la SSI (Gerber et Solms 2005).

La législation, selon Mcfadzean et al. (2007) concerne les codes de bonne pratiques, la conformité, les assurances et les standards et normes de sécurité. S'agissant des réglementations, Mcfadzean et al. les mentionnent dans deux facteurs, environnement et législation. Selon nous, il est nécessaire de distinguer la législation comme facteurs externes et non adaptables, auxquels il n'est pas possible de se substituer (cf. « 2.4.5 Conformité » section « Conformité réglementaire et légale » p. 72), des normes et standards dont l'application est propre à chaque entrepris et dont la littérature SSI démontre précisément

les difficultés de mise en œuvre (Barlette et Fomin 2010, cf. « 2.4.5 Conformité » section Conformité aux règles p. 71).

Ainsi Mcfadzean et al. étudient ces facteurs selon la perception des risques et les objectifs de l'organisation dont ils dressent une grille de perception (cf. Figure 19)

		Aim of Organisation	
		To Use ICT as an Operational Tool	*To Use ICT as a Source of Competitive Advantage*
Perception of Risk		**Operational Uncertainty**	**Strategic Uncertainty**
High	*Contextual Factors:*	Competitors not seen to be using IS aggressively	Competitors seen to be using IS aggressively
		Stakeholders' demand for security is high	Stakeholders' demand for security is high
		High internal and external threats	High internal and external threats
		Information security not serving needs of business	Existing security practices seen to be unsuccessful
	Board of Directors:	High perception of risk	High perception of risk
		Aim of organisation: To use ICT to support operations	Aim of organisation: To use ICT as a source of competitive advantage
		Budget for security is high (cost of security incidents seen as high)	Budget for security is high (cost of security incidents seen as high)
	Org. Action:	Managers articulate the enhancement of security	Managers articulate maximum security
		Managers intend that the new security strategy will change current operational business processes	Managers intend that the new security strategy will enable radical change to the current business processes
		Establish new security policies and procedures to accommodate change in security	Establish new security policies and procedures to accommodate transformation in security
		Operational Stability	**Strategic Stability**
Low	*Contextual Factors:*	Competitors not seen to be using IS aggressively	Competitors not seen to be using IS aggressively
		Stakeholders' demand for security is low	Stakeholders' demand for security is low
		Low internal and external threats	Low internal and external threats
		Existing security practices useful and successful	Existing security practices seen to be useful and successful
	Board of Directors:	Low perception of risk	Low perception of risk
		Aim of organisation: Use ICT to support operations	Aim of organisation: Use ICT as a source of competitive advantage
		Budget for security is low (cost of security incidents seen as low)	Budget for security is low (cost of security incidents seen as low)
	Org. Action:	Managers articulate minimal cost for security	Managers articulate minimal cost for security
		Managers intend that the new security strategy will preserve current business processes but ensure compliance	Managers intend that the new security strategy will preserve current business processes but ensure compliance
		Modify security policies and procedures to accommodate change in security	Modify security policies and procedures to accommodate change in security

Figure 19 : Grille de perceptions des risques et importance stratégique des SI

(Mcfadzean et al. 2007 p. 649)

Notons que, selon McFadzean et al. (2007), les top-managers ne développent pas eux-mêmes la stratégie de défense de leur SI mais valident celle proposée par des collaborateurs, bien que les premiers admettent des échanges difficiles avec les seconds. En effet le langage technique des spécialistes en SSI freine les top-managers qui, de plus, la considèrent comme une problématique opérationnelle qu'il faut déléguer (McFadzean et al. 2007). Ainsi, ils notent le potentiel développement **d'un faux sentiment de sécurité** des top-managers par « un manque d'alignement avec la stratégie globale de l'organisation » pouvant conduire à la mise en œuvre hâtive de solutions trop restreintes (telles que des pare-feux ou des antivirus) alors que ces « ces solutions miracles peuvent faire plus de mal que de bien » et que « leur gestion est devenue un cauchemar logistique » (McFadzean et al. 2007 p. 654).

En conclusion des travaux de McFadzean et al. (2007) nous retenons leurs apports sur la relation entre SI, risques et mise en œuvre des mesures SSI. Particulièrement, ils ont exposé les possibles relations entre les facteurs contextuels de l'entreprise, la perception des risques SI, et rôles institutionnels précisant les orientations des dispositifs de sécurité. Si McFadzean et al. étudient le risque et la perception des risques, la théorie sur ces deux concepts est peu développée. En effet, ils précisent le risque comme la possibilité que « leur entreprise soit exposée à des menaces externes et internes » et considèrent des risques techniques tels que la communication du mot de passe, « le vol, déni de service, virus ou corruption de donnée » (McFadzean et al. 2007 p. 638). Selon nous, cette définition du risque soulève deux commentaires. D'une part, elle reflète une vision partielle du risque telle que défini dans la littérature, autant dans le champ psychologique que SI, combinant une menace et une probabilité de perte (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Dhillon et Kayworth et Whitten 2010 ; Loch et al. 1992 ; Straub et Welke 1998 ; Torkzadeh 2006). D'autre part, cette approche technique du risque ne permet pas une communication adaptée avec les top-managers. En effet, rappelons que pour plusieurs auteurs en SSI, les pertes étudiées lors de l'analyse de risque au niveau gouvernance de l'organisation relève de **diverses conséquences négatives** telles que la perte de part de marché, l'incapacité de respecter des lois et des règlements, des pertes monétaires, et la perte d'image ou de réputation (cf. « 2.4.1 Gouvernance » p. 41, Fomin et al. 2010 ; Eloff et Solms 2000 ; Höne et Eloff 2002b ; Ma et al. 2008 ; Posthumus et Solms 2004 ; Solms et

Solms 2005 ; Straub et Welke 1998). Enfin, selon nous, leur étude ne traite pas de perception des risques au sens de Fischoff et al. (1981) ou Slovic et al. (1987) mais plutôt d'un niveau global de risque lié aux objectifs de l'organisation et niveau d'utilisation stratégique du SI, ne permettant alors pas d'identifier précisément quelle est la nature de l'influence de ces risques ont sur les rôles institutionnels.

Albrechtsen et Hovden (2009), le clivage entre managers SSI et les utilisateurs

Albrechtsen et Hovden (2009) éprouvent la déclinaison SSI du constat de Slovic (2000) selon lequel les facteurs de risques considérés par les profanes sont différents de ceux observés par les experts. Précisément, Albrechtsen et Hovden (2009 p. 476) indiquent qu'un « clivage numérique existe entre ces groupes en termes d'avis et d'expérience sur les pratiques de sécurité de l'information ». Sur la base de ce constat ils étudient la différence de point de vue entre managers et utilisateurs. Ainsi, ils soulignent que la divergence d'interprétation peut relever de caractéristiques individuelles, notamment les compétences et les connaissances pour la SSI, autrement appelées idiosyncratiques par d'autres auteurs (Karyda et al. 2005 ; Willison et Backhouse 2006), les perceptions de sécurité de l'information et des mesures de sécurité, les normes sociales et des relations interpersonnelles (Albrechtsen et Hovden 2009).

Ils ont demandé à 87 managers et 151 utilisateurs d'évaluer le niveau de risque en regard des « vulnérabilités / menaces » pour le SI dans leur fonction quotidienne au sein de leur organisation (Albrechtsen et Hovden 2009 p. 485) afin d'identifier les possibles différences de point de vue. Leurs résultats montrent une surévaluation des vulnérabilités spécifiques aux utilisateurs par les managers SSI telles que la négligence, les tentatives de social engineering, ou encore ne pas verrouiller son poste. Si Albrechtsen et Hovden exposent des possibles explications à ces différences de vues telles que le manque de compétences et de connaissances des utilisateurs, il permet de renforcer la position des managers SSI qui considèrent que les utilisateurs sont eux-mêmes une menace pour le SI. Notons que ces possibles raisons peuvent justement être corrigées par une meilleure communication et formation des utilisateurs par les managers SSI (Albrechtsen et Hovden 2009), reportant alors une part de vulnérabilité sur ces derniers. En ce sens, nous rejoignons justement le commentaire d'Albrechtsen (2007) qui, citant Slovic (2000), souligne l'amélioration potentielle pour la SSI lorsque les experts et profanes d'une même organisation approfondissent leurs visions des risques et des mesures de sécurité possibles. Les

utilisateurs, quant à eux, ont une forte aversion pour les menaces qui perturberait leur travail, comme le spam et l'utilisation imprudente d'Internet et des matériels » indiquant que les utilisateurs « sont plus égocentriques dans leurs évaluations », privilégiant les conséquences pour eux-mêmes en cas de dysfonctionnements (Albrechtsen et Hovden 2009 p. 486).

Si Albrechtsen et Hovden (2009) mobilisent les travaux de Slovic (2000), Sjöberg (2002) et Douglas et Wildavsky (1983), leur étude est **silencieuse sur les conséquences pour les interviewés ou sur l'organisation**. Précisément, ils étudient non pas les risques mais les « menaces et vulnérabilités » sur le SI telles que l'erreur humaine, les infections virales, la négligence, la mauvaise utilisation ou la perte d'information sensible, l'utilisation imprudente des mails, les vulnérabilités logicielles, l'utilisation imprudente d'Internet, l'utilisation du SI à des fins privées, l'ingénierie sociale, le spam, le piratage informatique, le vol de matériel / logiciel, et enfin, l'utilisation à des fins illégales (Albrechtsen et Hovden 2009 p. 485). Cette description montre que, selon les auteurs eux-mêmes, menaces et vulnérabilités sont évaluées indifféremment bien que ces deux concepts ne recouvrent pas les mêmes notions[53] alors que les auteurs mobilisent une définition du risque pour les organisations (op. cit.).

Plus globalement, selon nous, cette conception du risque **selon les menaces et les vulnérabilités peut justement éclairer la différence de vision entre utilisateurs et managers**, les premiers centrés sur les risques SI auxquels ils seraient exposés et provoquant un incident sur leur propre fonction « métier », alors que les seconds considèrent davantage les menaces techniques exposant le SI, rejoignant alors une vision techno-centrée de la SSI, décriée par plusieurs auteurs (Dhillon et Backhouse 2001 ; Karyda et al. 2005 ;Kayworth et Whitten 2010 ; Spears et Barki 2010). En ce sens, Albrechtsen (2007) relève justement que les utilisateurs se concentrent prioritairement sur le cœur de leur fonction plutôt que sur les mesures de sécurité du SI[54]. Ainsi, nous suggérons qu'une approche du risque telle que définie dans la littérature SSI et recouvrant à la fois l'exposition au risque, soit la probabilité, et les conséquences pour l'organisation et l'individu aurait éclairé une possible divergence de vision du risque entre experts (managers SSI) et profanes, (utilisateurs).

[53] Cf. Magne (2010) pour la notion de menace en perspective des dommages, Loch et al. (1992) pour les menaces SI et Willison et Backhouse (2006) pour les vulnérabilités SI

[54] Selon une stratégie de satisficing telle que développée par March et Simon (1958, cf. Albrechtsen 2007 p. 277)

Huang et al. (2010), perception de sécurité de l'information

Huang et al. (2010 p. 224) ont examiné les facteurs qui peuvent influencer les risques SI de répondant « qui ont de l'expérience sur l'usage de PC sur Internet ». En appuyant leur étude sur le cadre théorique du paradigme psychométrique (Fischhoff et al. 1978 ; Slovic et al. 1987) ils ont développé une grille de perception de risque spécifique à la SSI sur la base d'une revue des travaux académiques[55] desquels ils ont extraits puis articulés 20 déterminants (cf. Figure 20). Ils ont ensuite étudié leur influence sur la perception de la sécurité de l'information de 602 répondants. Si les déterminants du risque sont comparables aux travaux de Fischoff al. et Slovic et al., le regroupement en facteur diffère, Huang et al. (2010) définissent 6 facteurs de la façon suivante :

1. « connaissance »: caractère familier, compréhension, contrôle de sévérité et nouveauté. Ces déterminants sont liés à la connaissance des menaces. Si les individus ne sont pas familiers avec ces menaces, la compréhension de leur sévérité et les possibilités de les contrôler ne sont pas facile à appréhender (op. cit).
2. « impact » : durée des impacts, la portée des impacts et attention médiatique. Les individus sont davantage concernés par des menaces qui durent, dont la portée est importante et qui sont exposées médiatiquement
3. « sévérité » : exposition personnelle, le volontarisme et sévérité des conséquences. La perception des menaces prend en compte le sérieux des menaces, l'exposition volontaire à ces menaces et l'ampleur des conséquences pour la société
4. « contrôlabilité » : mesure préventive, observable, facilité de réduction (des conséquences), réversibilité, prévisibilité et potentiel catastrophique. Ce facteur indique dans quelle mesure les menaces peuvent être contenues
5. « possibilité de survenance » : exposition antérieure, possibilité de survenance de cette menace
6. « conscience » : immédiateté de l'effet et connu.

[55] La revue de la littérature mobilisée par Huang et al. 2010 met en évidence x travaux dans le champ de la SSI : Gonzalez et Sawicka 2001 ; Thomson et von Solms 2005 ; Gorden et al. 2006 ; Whitman, (2003, 2004) ; Vyskoc et Fibikov (2001)

Items	Description in the survey
1. Familiarity	I am familiar with this threat.
2. Severity of consequences	The consequences of this threat are serious.
3. Voluntariness	I am exposed to the risk of this threat voluntarily.
4. Catastrophic potential	The outcomes of this threat are grouped in time and space (instead of being scattered in time and space).
5. Understanding	I understand this threat.
6. Personal exposure	This threat causes personal harm (instead of public harm).
7. Observability	This threat is observable.
8. Ease of reduction	The effect of this threat can be reduced easily.
9. Preventive control	This threat can be prevented.
10. Control of severity	The severity of the effect of this threat can be controlled.
11. Immediacy of effect	The effects of this threat are apparent immediately.
12. Known to those exposed	The existence of this threat can be known to those exposed to it.
13. Newness	This threat is a new or novel one.
14. Media attention	The media pays much attention to this threat (media such as newspapers, TV and Websites).
15. Accident history	I have never been exposed to this threat.
16. Reversibility	The effect of this threat can be reversed.
17. Duration of impacts	The duration of the impacts of this threat is long.
18. Scope of impacts	The scope of the impacts of this threat is wide.
19. Predictability	This threat can be predicted.
20. Possibility	The possibility that I will be exposed to this threat is large.

Figure 20 : Grille des déterminants qui peuvent influencer la perception des risques SI

(Huang et al. 2010 p. 224)

Les menaces potentielles, telles que par exemple, des virus, des pirates, le fishing, la fraude, … ont été étudiées comme menaces redoutées, faisant émerger sept déterminants (sévérité des conséquences, portée des impacts, exposition antérieure, volontarisme, durée des conséquences, compréhension et possibilité de survenance). Ainsi, les facteurs qui, selon Huang et al. (2010 p. 227) caractérisent le mieux « le danger perçu » sont la « sévérité » (3),

l'impact (2), la possibilité de survenance (5) et la « connaissance » (1). En ce sens, les résultats semblent se distinguer des travaux de Slovic et al. 1987 par l'absence des facteurs de « contrôlabilité » et de « conscience » de Huang et al. (2010). Ceci peut s'expliquer, selon nous, par la définition mobilisée du risque perçu par les individus. En effet, le concept de risque n'est que partiellement retenu au profit de « menace », en notant que les auteurs emploient parfois le terme « danger ». Cela peut alors modifier substantiellement la façon d'aborder la perception du risque, pour laquelle Fischhoff et al. (1978) et Slovic et al. (1987) ne font aucune ambiguïté. Ainsi, dans un second temps, Huang et al. étudient l'« effet du type de perte » pour mettre en évidence l'aversion pour la perte financière et le désagrément potentiel causé par la menace, en dissociant la perte de la menace. Les auteurs expliquent **ces raisons par la nature culturelle des répondants qui sont des « utilisateurs chinois »** Huang et al. (2010 p. 230).

En synthèse, Huang et al. (2010 p. 231) ont conduit « une étude exploratoire visant une meilleure compréhension de la perception des individus pour la sécurité de l'information ». Dissociant la menace de la perte, ils ont, de notre point de vue, biaisé le concept de risque tout en mobilisant des travaux princeps de Fischhoff et al. et Slovic et al.. Si l'objet nous parait tout à fait intéressant, améliorer la connaissance de la perception des risques SI des individus, l'étude du risque doit être contextualisée comme le martèlent plusieurs auteurs (Sjöberg et al. 2004 ; Yates et Stone 1992). En ce sens, rappelons que l'étude de la perception des risques concerne l'acceptabilité, qui fait interagir plusieurs spécificités de l'évaluateur et du risque telles que l'appétence au risque, les bénéfices perçus, le contexte et les enjeux de la situation risquée. Cette approche de l'étude des risques ne peut alors s'affranchir des conséquences possibles dans un contexte de situation risquée définie.

Synthèse des travaux SSI sur la perception des risques

Afin de disposer d'une vision globale des huit travaux académiques mobilisant la perception des risques, nous établissons une synthèse précisant le sujet, la théorie mobilisée et les principaux apports.

Auteurs	Sujet	Théorie mobilisée	Objet étudié	Principaux apports
Loch et al. 1992	Comment sont perçues les menaces internes et externes, humaines et naturelles et lesquelles sont les plus importantes (pour microcomputers, mainframes et réseaux)	/	Managers SSI	Ambiguïté entre exposition perçue élevée aux menaces et niveau de risque faiblement évalué
Straub et Welke 1998	Les managers perçoivent la sécurité selon leur 1) croyance de l'exposition de l'industrie au risque, 2) les actions SSI entreprises au sein de leur organisation et 3) leurs caractéristiques individuelles (sensibilisation, connaissance des mesures, expérience)	Théorie générale sur la dissuasion (Straub et Welke 1998)	Managers	Définition d'un modèle de gestion des risques qui fait interagir les managers et les spécialistes SSI
Taylor 2006	Perception des risques des managers en regard des mesures organisationnelle en place	Perception des risques (Fischhoff et al. 1978)	Managers	Mise en exergue d'un faux sentiment de sécurité porté par les spécialistes SSI ; ¡Ils ne tiennent pas compte des risques globaux mais des risques technologiques
Tsohou et al. 2006	Effet de la théorie culturelle sur la perception des risques et les décisions de les traiter	Théorie culturelle (Douglas 1978 ; Douglas et Wildavsky 1983).	Utilisateurs non caractérisés dans l'étude	Éclaire théoriquement la perception des risques selon les biais culturels ainsi que l'influence sur la méthode d'analyse et de traitement des risques SI
Albrechtsen 2007	Les utilisateurs s'impliqueront davantage dans la SSI s'ils en comprennent les raisons (risque)	Homéostasie du risque (Wilde 1982) Culture du risque (Douglas et Wildavsky 1983) Perception (Slovic 2000)	Utilisateurs finaux	Nécessité de comprendre les risques pour adopter un comportement adéquat, la faiblesse de la protection s'appuie sur le manque de connaissance des risques et des conséquences
McFadzean et al. 2007	Influence des risques perçus sur les rôles des directeurs	Grounded theory La théorie de la structuration (Giddens 1984)	Managers	Influences du rôle stratégique du SI et du contexte de l'organisation sur les risques perçus et les solutions pour y répondre
Albrechtsen et Hovden 2009	Différence de vision SSI entre managers et utilisateurs en regard de leur expérience et pratiques de sécurité	Homéostasie du risque (Wilde 1982), perception des risques (Slovic 2000), théorie culturelle du risque (Douglas et Wildavsky 1983)	Utilisateurs finaux	Dualité entre vision experts / profanes, ils n'investissent pas les mêmes problématiques ; Besoin de communication entre les individus de l'organisation pour une SSI adaptée
Huang et al. 2010	Comparaison de la perception des menaces SI les plus sévères avec les moins dangereuses	Perception des risques (Fischhoff et al. 1978 ; Slovic et al. 1987)	Utilisateurs non caractérisés dans l'étude	Déclinaison des déterminants du paradigme psychométrique des risques sociétaux aux menaces SI

3.2.8. Synthèse du chapitre sur la perception des risques

La littérature fait consensus lorsqu'il s'agit de définir la SSI comme une discipline de gestion du risque (Bandyopadhyay et al. 1999 ; Doherty et Fulford 2006 ; Siponen et Oinas-Kukkonen 2007 ; Solms et al 1994 ; Wood 1995) dont les arbitrages doivent être opérés au plus haut niveau des organisations (Hu et al. 2007 ; Posthumus et Solms 2004 ; Kayworth et Whitten 2010). Le concept de risque mobilisé en SSI rejoint complètement celui de la psychologie, soit la probabilité d'un évènement indésirable et l'ampleur de ses conséquences (Amalberti 1996 ; Bandyopadhyay et al. 1999 ; Dhillon et Torkzadeh 2006 ; Fischoff et al. 1978 ; Slovic et al. 2004 ; Sjöberg et al. 2004). Cette conception du risque constitue la base des modèles de risque étudiés dans ce chapitre.

Ainsi, attendu que la SSI relève pleinement de la gestion des risques SI et que notre projet vise à explorer les influences sur l'adoption symbolique de la SSI par les top-managers, le risque, sa perception et son acceptation s'y inscrivent pertinemment. En effet, selon Kermisch (2012) la discipline de gestion du risque dans le champ psychologique offre une définition multidimensionnelle du risque et une approche conceptuelle riche pour établir la **représentation retenue par les individus et leur réponse**. Enfin, l'acceptation du risque dont plusieurs auteurs soulignent qu'il s'agit de la combinaison du bénéfice attendu et du risque perçu (Cadet et Kouabénan 2005 ; Fischhoff et al. 1981). C'est justement les éléments permettant de définir le risque comme acceptable que nous souhaitons étudier pour la décision de protéger le SI. En ce sens, rappelons que Solms (2006) caractérise comme décision la réponse de l'entreprise sur les dispositions prises pour atténuer les risques ayant un impact sur le SI. La perception des risques est alors une influence incontournable dans la décision pour les traiter car, comme l'indiquent Fischhoff et al. (1978) et Slovic et al. (1980) **ce qui est en dehors de la vue est en dehors de l'esprit,** suggérant que seuls les risques perçus peuvent être considérés, avant même d'évoquer la décision de les traiter. Il s'agit alors de considérer dans notre étude, **la connaissance des risques par les top-managers** d'une part, et les **réponses que ces derniers pourraient y apporter** en termes de SSI.

La littérature sur la perception des risques, en regard des travaux sur la SSI, renforce la pertinence d'étudier la décision d'adopter symboliquement la SSI. En effet, la décision quant à SSI nécessite de **mobiliser le concept de risque dans sa globalité**, ne pas considérer isolément une menace ou une vulnérabilité du SI mais davantage **la probabilité de pertes** pour l'entreprise. Par exemple, Magne (2010) précise qu'un ours est une menace pour

l'Homme à condition d'en être proche et lorsqu'il est n'est pas dans une cage. Naturellement, le risque relève alors de la **probabilité d'être atteint physiquement** par un ours dont l'Homme serait à proximité. Ainsi, le risque s'efface dès lors que les conditions ne sont pas réunies. En d'autres termes, ce risque ne peut se formuler par la seule menace, « il y a des ours » ou la seule conséquence, « être blessé par un ours ». En ce sens, Liang et Xue (2009) soulignent que l'évaluation de la réponse survient **lorsque la menace est perçue** comme pouvant empêcher le décideur d'atteindre ses objectifs, en accord avec Fischhoff et al. (1978) et Slovic et al. (1980). Ils précisent alors que l'évaluation d'un risque SI est effectué selon un processus en deux parties : 1) l'évaluation de la menace ; 2) l'évaluation de la réponse possible à cette menace (Liang et Xue 2009)

Ainsi, comprendre les influences sur la décision quant au risque implique d'appréhender la perception du risque en rappelant qu'il est situationnel, contextuel et subjectif. **Situationnel** parce que l'évaluation ne s'affranchit pas des conditions et de l'environnement dans lesquels l'évaluateur construit sa réflexion pour accepter, ou non, le risque (Sjöberg et al. 2004 ; Yates et Stone 1992). **Contextuel** car l'évaluateur mobilise des informations propres à son organisation telles que les compétences pour le risque SI, les processus pour les maitriser (Backhouse et Dhillon 1996 ; Dhillon et Backhouse 2001 ; Straub et Welke 1998) ou encore la culture sécurité (Douglas et Wildavsky 1983 ; Hagen et al. 2008 ; Sjöberg et al. 2004 ; Rippl 2002 ; Tansey et O'riordan 1999). Slovic et al. (1979) indiquent que les sources différentes d'informations de l'évaluateur sont mobilisées pour élaborer des inférences qui alimenteront l'évaluation et l'acceptation du risque, en complément de ses enjeux et objectifs (Sjöberg et al. 2004), rendant le risque **subjectif**.

Cadet et Kouabénan (2005) comparent les différents paradigmes pour évaluer et modéliser le risque et concluent que l'utilité espérée vise à définir un risque acceptable, le paradigme psychométrique permet d'évaluer et de comparer des risques perçus par des groupes sociaux, et le paradigme cognitif fait émerger les modalités de traitement de l'information qui conduisent à l'acceptation ou au rejet. Nos travaux ne s'inscrivent pas dans la perspective d'évaluer, de comparer ou d'étudier les modalités de traitement de l'information mais d'explorer les influences sur l'adoption symbolique de la SSI. Le concept de risques est alors étudié **comme influence possible de la décision quant à la SSI**, telle que rappelé par plusieurs auteurs (Albrechtsen et Hovden 2009 ; Choobineh et Dhillon 2007 ; Goodhue et Straub 1991 ; Taylor 2006 ; Kotulik et Clark 2004). Pour cette raison, nous n'écartons aucun des paradigmes présentés, quand bien même le paradigme psychométrique englobe un cadre théorique qui assume que le risque soit subjectivement défini par les individus qui

peuvent être influencés par un large tableau de facteurs psychologiques, sociaux, institutionnels et culturels (Kermisch 2010 ; Sjöberg et al. 2004). En effet, les études mobilisant le paradigme psychométrique font émerger des préférences et aversions pour des risques potentiels en regard de caractéristiques individuelles (Slovic et al. 1984). Kermisch (2010 p. 48) souligne que ce paradigme permet l'étude de la manière dont sont perçus les risques inhérents à différentes activités, substances ou technologies », en adéquation avec notre projet de situer le risque comme une influence à l'adoption symbolique de la SSI.

Dans la littérature mobilisée dans nos travaux émerge aussi l'importance des influences sociales du risque et de l'environnement, que ce soit pour la perception du risque (Douglas et Wildavsky 1983 ; Sjöberg et al. 2004), pour la décision (Klonglan et Coward 1970 ; Sapp et Korsching 2004), ou pour la SSI (Hu et al. 2007 ; Kwon et Johnson 2014). En effet, rappelons l'importance des influences sociologiques sur la décision, particulièrement à la seconde étape de l'AS, lorsque les individus s'informent et se renseignent sur l'innovation, durant laquelle l'influence informationnelle et normative intervient principalement (Karahanna et al. 1999). Pour Rippl (2002) et Sjöberg et al. (2004), les facteurs sociaux et institutionnels influent sur l'évaluation des risques (Sjöberg et al. 2004). Enfin, Hu et al. (2004) soulignent l'importance de la théorie néo-institutionnelle pour aborder les influences coercitive et normative pour la SSI, et pour Dlamini et al. (2009 p. 2) les organisations mettraient en œuvre la SSI « simplement parce que toutes les autres le font »

Nous prolongeons alors l'analyse de la littérature en définissant, dans la section suivante, les possibles influences externes et internes sur la décision d'adopter symboliquement la SSI sur la base de la théorie néo-institutionnelle (Di Magio et Powell 1983 ; Scott 2005).

3.3. Influences externes et internes

Di Maggio et Powell (1983) présentent la théorie de l'isomorphisme institutionnel comme une influence d'homogénéisation structurelle ou de standardisation des organisations pour renforcer leur légitimité. En effet, « dans le même champ, les organisations qui produisent des services ou des produits similaires, qui partagent des fournisseurs, des ressources ou des clients identiques, sont sujettes à des pressions institutionnelles, internes et externes, similaires » (Lesca et al. 2015 p. 13). Selon Scott (2005), les organisations sont des systèmes sociaux dont la théorie néo-institutionnelle permet justement d'expliquer leurs actions en réponse à la pression environnementale, légitimant son utilisation « pour répondre aux

questions concernant le rôle d'influence institutionnelle sur des choix sociaux » (Williams et al. 2009 p. 596).

Si la théorie institutionnelle traite les formes, les schémas, les règles, les normes et les routines des organisations, nous pouvons également la mobiliser lorsque l'individu représente l'unité d'analyse (Scott 2005). Par exemple, Karahanna et al. (1999), montrent que l'adoption d'une technologie s'effectue selon 2 éléments, soit l'intérêt personnel et l'influence sociale. Swanson et Ramiller (2004 p. 556) précisent que si l'innovation technologique est réalisée au niveau organisationnel, cette forme de vision d'organisation se définit comme « une idée communautaire focale pour l'appliquer dans des organisations » dont **la communauté repose aussi sur les individus**. En ce sens Lesca et al. (2015), lorsqu'il s'agit d'adopter des innovations technologiques, indiquent l'émergence des idées et des discours au sein de communauté professionnelle. Ainsi, l'isomorphisme institutionnel peut combiner dans le même temps un discours normatif et des influences que les organisations et les acteurs exercent les uns sur les autres. Liang et al. (2007 p. 61) prolongent ce constat en indiquant que « les forces externes, aussi fortes soient-elles, n'auront aucun effet sur le comportement d'une organisation sans affecter d'abord le **comportement des acteurs** dans l'organisation ».

Particulièrement, notons que Hu et al. (2007) s'appuient sur l'appel de Dhillon et Backhouse (2001) à considérer la sécurité sous l'angle socio-organisationnel pour mobiliser la théorie néo-institutionnelle. Hu et al. (2007 p. 156) suggèrent alors « que la théorie néo-institutionnelle est adaptée pour expliquer comment les facteurs institutionnels externes influencent le comportement des acteurs de l'organisation et ainsi le comportement de l'organisation » elle-même. Si la littérature en sécurité compte peu d'articles sur les études d'adoption mobilisant la théorie néo-institutionnelle, à notre connaissance, deux sont notables. Le premier vise à identifier les facteurs institutionnels externes et internes prégnants pour la SSI et comment ils alimentent la connaissance des top-managers et des collaborateurs (Hu et al. 2007). Le second, dans le champ de la sécurité logistique, vise à comprendre les motivations des organisations à engager des pratiques de sécurité de la chaine logistique (Williams et al. 2009).

Pour la théorie de l'isomorphisme institutionnel, l'homogénéisation des organisations et leurs structures, processus, comportements ou culture, s'explique par trois formes d'isomorphismes, soit l'isomorphisme coercitif, l'isomorphisme normatif et l'isomorphisme mimétique.

3.3.1. Isomorphisme coercitif

L'isomorphisme coercitif est le résultat de pressions au sens large, formelles ou informelles, exercée par les organisations d'un même champ, qui favorisent l'adoption de normes communes (Di Maggio et Powell 1983). L'influence de l'État est évidente, par exemple à travers la promulgation de nouvelles règlementations, obligeant les organisations à s'adapter et innover (Lesca et al. 2015 ; Rizza 2008). Ces pressions institutionnelles coercitives prennent souvent la forme de lois ou de de règlements, les organisations l'adoptent aussi pour éviter les pénalités et les sanctions (Scott 1995). Pour Williams et al. (2009 p. 598) ces influences peuvent aussi être issues de ceux qui « ont la capacité d'exercer des pressions formelles et informelles, telles que des clients et des fournisseurs. Cette influence a un caractère incontournable pour les organisations qui y sont exposées, les contraignant à adopter ces structures spécifiques pour obtenir une légitimité, dont le corolaire est caractérisé par des processus produisant l'homogénéité. En effet, selon Rizza (2008), à l'appui des travaux de March (1991), les acteurs préfèrent adosser leur décision à des « conditions déjà expérimentées » et « tenues pour sûres ». En ce sens Kwon et Johnson (2014 p. 455) précisent que plusieurs études « ont constaté que les pressions externes sont importantes pour l'apprentissage organisationnel » parce qu'elles permettent aux organisations **d'explorer préventivement certains problèmes** et d'éviter les échecs futurs, en s'appuyant sur des modes d'actions déjà éprouvés. Cet argument soutient l'idée que les pressions réglementaires peuvent stimuler l'apprentissage organisationnel et le changement car elles astreignent les acteurs des organisations à prêter plus d'attention aux échecs, à les analyser pour empêcher qu'ils ne surviennent à l'avenir (Kwon et Johnson 2014).

Nous pouvons faire le parallèle avec la notion de connaissance du risque développé par Fischoff et al. (1978) et Slovic et al. (1979) qui soutiennent qu'un risque, ici un potentiel échec, peut être analysé et traité dès lors qu'il est connu, quelle que soit la source d'information. En ce sens Hu et al. (2007 p. 165) soulignent les effets significatifs de « la pression réglementaire telle Sarbanes-Oxley et les résultats négatifs d'un audit » (sur la SSI) qui ont conduit les top-managers de l'organisation étudiée à « instituer des réformes pour la sécurité des systèmes d'information ». Précisément, c'est la « crainte d'un audit » externe diligenté par les autorités de régulation de SOX après un potentiel incident (vol de numéros de carte de crédit) qui ont accéléré la formalisation des procédures de SSI de cette organisation (Hu et al. 2007 p. 162). Kwon et Johnson (2014) soulignent les effets de la

réglementation et des normes spécialisées sur les mesures SSI proactives mises en œuvre, réduisant le nombre d'incidents. Dans la même perspective, pour la sécurité des chaines d'approvisionnement, Williams et al. (2009) concluent que les entreprises logistiques aux États-Unis ont adopté les pratiques recommandées « fortement » par les autorités compétentes en termes de sécurité, afin de ne pas être exposées à des contraintes spécifiques qui auraient pu limiter ou réduire leurs activités de transports. Ces entreprises ont également répondu favorablement à ces exigences car elles ont mesuré le risque social liées à leurs activités. Par exemple, une entreprise spécialisée dans le transport de colis a souscrit à ces mesures pour ne pas être celle qui « aurait transporté un colis piégé qui aurait eu des impacts désastreux sur des personnes innocentes » (Williams et al. 2009 p. 607). Si Williams et al. (2009) démontrent l'effet de l'isomorphisme dans ce cas, ils évoquent la difficulté de le distinguer de l'isomorphisme normatif, dont un des constats est justement l'impact sur la société au sens de nation.

Kwon et Johnson (2014) suggèrent que les démarches proactives et volontaires sont associées à une meilleure performance que celles initiées par la pression externe. Ils émettent toutefois la réserve que si la pression réglementaire peut fournir des directives de résolution de problèmes, l'apprentissage organisationnel induit nuit partiellement à l'effet de l'apprentissage autonome de la prise de décisions proactive. Précisément, sous la pression externe une organisation peut passivement essayer de respecter les exigences d'un règlement ou d'une loi plutôt que de conduire activement sa propre analyse de problème et de solution. En d'autres termes, ce constat peut rejoindre celui établi par plusieurs auteurs à l'endroit des normes pour la SSI (cf. « 2.4.5 Conformité » p. 70), qui indique l'absence d'adaptation de l'organisation des mesures standardisées, ne traitant pas des risques spécifiques à l'organisation (Solms 2000) conduisant à des mesures de sécurité génériques, aboutissant potentiellement à des investissements inopportuns (Siponen et Willison 2009 p. 268) et écartant de la vision globale des risques les activités majeures particulièrement exposées, présentant alors une représentation « déformée » de la sécurité (Willison et Backhouse 2006).

3.3.2. Isomorphisme normatif

L'isomorphisme normatif se rapporte **aux pressions exercées par les organisations professionnelles et les réseaux associatifs**, soit l'ensemble des efforts collectifs d'une profession pour définir leurs compétences et leurs méthodes de travail (Scott 1995). Alors

que dans une même organisation les métiers sont différents les uns des autres, ils sont très similaires aux métiers des organisations homologues (Di Maggio et Powell 1983). Pour ces auteurs, les groupes professionnels jouent un rôle de facilitateur dans la **diffusion de nouvelles connaissances**, mais exercent également des pressions normatives (op. cit.). Deux sources d'isomorphisme normatif sont identifiables. L'une traite de la standardisation des cursus éducatifs, concourant à réunir des « managers formés dans les mêmes instituts de formation et faisant souvent partie de communautés professionnelles, partageant des croyances semblables sur la « juste manière d'organiser » (Rizza 2008 p. 13). L'autre relève de réseaux sociaux professionnels dans lesquels les membres développent une culture commune conduisant aussi à l'homogénéisation. Précisément, les décisions professionnelles de ces membres s'inscrivent dans un comportement d'adoption des normes et techniques les plus adéquates du domaine pour ne pas se distinguer des pratiques du marché, au risque de s'en exclure (Rizza 2008).

Dès lors que l'on considère des **valeurs, des croyances et une culture commune**, nous pouvons évoquer ces concepts en perspective de la théorie culturelle du risque. Précisément, nous rappelons justement **qu'en situation d'incertitude**, les styles de pensée régissent l'action sociale des individus tels que décrits Douglas et Wildavsky (1983). En effets, les valeurs partagées se combinent dans certains contextes sociaux et culturels, les biais culturels, pour former la **perception des risques des individus**. Dans un autre champ de la littérature, pour les travaux sur l'adoption symbolique, Sapp et Korsching (2004 p. 352) soulignent l'importance « des croyances normatives perçues » pouvant conduire à la décision d'adoption ou de rejet symbolique. Particulièrement au risque SI, rappelons que la perception des top-managers repose, selon Straub et Welke (1998), sur leurs croyances de l'exposition de leur organisation au risque, en tenant compte globalement des risques qui s'imposent à la même activité et donc aux organisations homologues[56]. McFadzean et al. (2007), précisent l'impact de ces influences sur la perception des risques mais aussi sur les rôles et les actions des managers. En ce sens, la connaissance des risques SI s'inscrit dans la subjectivité des top-managers, en regard de leurs croyances et des valeurs partagées avec leur réseau d'influence, dont le groupe professionnel peut faire partie, rejoignant alors la deuxième source d'isomorphisme normatif. Selon Di Maggio et Powell (1983), cette uniformité est autant le fait des échanges sur les pratiques et des forces isomorphiques que de l'absence de solutions innovantes accessibles pour résoudre une problématique donnée.

[56] Les deux autres sont les actions SSI entreprises au sein de leur organisation et leurs caractéristiques individuelles

En effet, en situation **d'incertitude**, la recherche de la solution optimale revient souvent à adopter **la première solution connue** (*satisficing*) telle que développé par March et Simon en (1958) et soulignée par Albrechtsen (2007) pour les options de traitement des risques SI. Hu et al. (2007) ont étudié comment ces influences externes et internes forment des actions organisationnelles pour améliorer la SSI. S'ils notent l'importance des réseaux professionnels sur la connaissance des mesures SSI des top-managers, ils constatent aussi une dynamique équivoque d'influence entre top-managers et utilisateurs (*top-down* et *bottom-up*), en accord avec les travaux de Scott (1995) sur l'influence ascendante. Hu et al. (2007) notent aussi que les influences externes motivent l'engagement de la direction générale pour la SSI plus fortement que des influences internes.

Williams et al. (2009) montrent l'influence de l'isomorphisme normatif sur les chaines d'approvisionnement suite aux mesures de sécurité recommandées par le législateur et assorti d'une autre influence, notamment vis-à-vis de la concurrence des autres entreprises, le mimétisme.

3.3.3. Isomorphisme mimétique

L'isomorphisme mimétique résulte « de l'incertitude et de la rationalité limitée face auxquels les organisations ont tendance à s'imiter entre elles » (Lesca et al. 2015). Pour les mêmes raisons évoquées ci-avant, l'absence de connaissance pour une activité incertaine peut conduire à l'imitation. Pour Lesca et al. (2015 p. 16), les organisations d'un même champ peuvent aussi s'imiter « entre elles pour être perçues comme plus légitimes ». Dans cette perspective, Dlamini et al. (2009 p. 2) font l'hypothèse que « pendant longtemps la plupart des organisations n'ont pas reconnu l'importance de sécuriser » leur SI car la sécurité était considérée « comme un mal nécessaire qui gêne la productivité », les organisations mettraient en œuvre la SSI « simplement parce que toutes les autres le font ».

Lorsqu'on observe les conclusions de Hu et al. (2007) elles ne s'articulent pas avec le principe même de l'isomorphisme mimétique. En effet, si le mimétisme est adossé à l'imitation d'un comportement dont le décideur sait qu'il est adapté à la situation, ce constat pour la SSI n'est pas adapté car justement, pour les mêmes auteurs, la définition d'une SSI réussie signifie que « rien n'est arrivé », elle n'est alors pas communiquée comme un succès, Kotulic et Clark (2004) rappelant qu'il s'agit par ailleurs d'un sujet confidentiel. Précisément Hu et al. (2007) soulignent le manque « d'histoires à succès » qui limite par construction la communication auprès des top-managers, se retrouvant ainsi en déficit d'information sur les

des pratiques qu'ils pourraient imiter. A l'inverse, Kwon et Johnson (2014 p. 455) dans le secteur médical, mettent en évidence le but visé par l'isomorphisme mimétique, la volonté de ne pas avoir à subir de perte d'image : « au cours de la dernière décennie, les lois de notification d'infraction ont exigé que des organisations notifient les propriétaires de l'information d'infractions de sécurité. Dans les services médicaux, les infractions créent souvent des réactions publiques exceptionnellement fortes à cause de la nature privée et confidentielles d'informations médicales ». Les lois imposant la notification d'infraction créent une pression organisationnelle significative, tant à cause du coût de notification qu'à cause de la couverture médiatique négative.

3.4. L'adoption symbolique adaptée à la gestion du risque

Notre objectif est de pouvoir considérer globalement la décision d'adopter symboliquement la SSI par les top-managers, présenté autrement, d'identifier et comprendre quelles sont les influences prises en compte pour répondre au besoin de protéger les SI de l'organisation par le potentiel adoptant. À cette fin, nous présentons un modèle adapté à la décision d'adopter symboliquement la SSI, en précisant, sur la base de différents champs de littérature, quelles seraient les influences qui pourraient être considérées dans chaque étape du modèle d'AS de Klonglan et Coward (1970).

3.4.1. Première étape : le besoin de protéger le SI

L'approche risque pour le SI, combinant menace et probabilité (Bandyopadhyay et al. 1999) peut **synthétiser les besoins de protection du SI**. D'une part, il s'agit de traduire en conséquences intelligibles et potentielles, selon des méthodes éprouvées, en quoi l'organisation et par extension les top-managers peuvent être **concernés par la survenance d'un risque**. Ainsi, à l'appui de la littérature, nous avons précisé que ces conséquences, pour justement être prises en compte dans une perspective « métier », ne se présentent pas en termes de risque SI. Il s'agit davantage de considérer les conséquences qu'auraient un risque **pour l'activité et le devenir** de l'organisation, dont, nécessairement le SI est un support aux processus majeurs. En synthèse, tel que décrit au paragraphe « 1.1.2 La protection des SI », les conséquences de définissent comme 1) des **pertes financières directes** (Bagchi et Udo 2003 ; Choobineh et Dhillon 2007 ; Ma et al. 2008 ; Straub et Welke 1998), 2) des pertes **économiques ou financières** (Bandyopadhyay et al. 1999 ; Baskerville

1993 ; Cavusoglu et al. 2004 ; Doherty et Fulford 2006), 3) des **pertes d'image** (Kayworth et Whitten 2010 ; Posthumus et Solms 2004 ; Solms 1999), 4) pouvant entrainer des **implications juridiques** (Eloff et Solms 2000 ; Höne et Eloff 2002b) et 5) **des impacts stratégiques** (Solms et Solms 2005).

Rappelons ici que le risque est par construction une combinaison d'éléments qui le rend **complexe** (Gerber et Solms 2005) et **abstrait** (Tsohou et al. 2006). Si pour Hu et al. (2007) une sécurité des SI réussie se définie par l'absence de conséquence et donc par des contre-mesures efficaces ou /et une absence de survenance du risque, Kwon et Johnson (2014 p. 452) soulignent que souvent, le risque SI n'est pas considéré tant que « rien n'est arrivé ». Par exemple, Herath et Rao (2009a), sur la base de travaux de la théorie de la motivation de protection (PMT) de Rogers (RW 1975 et 1983) développée pour comprendre comment **la crainte motive** le comportement vis-à-vis de la sécurité, ont soutenu que l'attitude pour l'adoption de la SSI est formée par **l'évaluation de menace et du succès du processus d'évaluation**. Ce commentaire renforce alors l'idée que l'évaluation et la perception du risque peuvent conduire à adopter des mesures de sécurité SI comme un moyen pour faire face à ces risques (Bulgurcu et al. 2010). Typiquement, Karyda et al. (2005), en accord avec Goodhue et Straub (1991), assoient la compréhension du besoin de SSI sur les **caractéristiques idiosyncratiques des décideurs**. Ainsi, Straub (1990) mentionne que la préoccupation pour la SSI des managers est justement **fonction du niveau de risque perçu** ce qui renforce l'interrogation développée au paragraphe 2.4.4 « Analyse de risque » (cf. « Gestion des risques : décision et responsabilités de la SSI »). En effet, la littérature souligne **l'analyse de risque comme première étape du processus permettant d'organiser la SSI** (Wood 1995), en objectivant les risques qui s'imposent, leur probabilité et conséquences. Il s'agit alors d'identifier quels risques sont considérés par les top-managers lors de cette étape de l'AS, qui conduirait à la décision d'initialiser la SSI et par conséquent, dans un second temps, l'analyse de risque en tant qu'étape formelle d'études des risques SI.

Cette première étape du processus d'adoption symbolique devrait permettre de rendre intelligible quels éléments le potentiel adoptant mobilise pour constituer *« la connaissance »* conduisant à l'AS de la SSI :

- le SI doit être sécurisé, par exemple sur la base d'un incident survenu (Kwon et al. 2012),
- un risque possible est « imaginé » et la décision de l'analyser est initiée (Straub 1990),

- la pratique de la SSI « apparait » dans le champ de connaissance (Doherty et Fulford 2006),
- la SSI est imposée à l'organisation (Knapp et al. 2009).

En synthèse, nous avons vu la relation étroite entre le risque, la gestion du risque et la SSI. Si la sécurité de SI est l'innovation à adopter qui conduira ensuite au processus formel d'analyse de risque, il **s'agit d'identifier l'émergence du besoin** chez les top-managers : volonté de répondre à des risques potentiels, de mettre en place la SSI en tant que concept, ou les deux en même temps ? Plus précisément et selon les indications du cadre théorique d'AS, il s'agit d'étudier la réflexion conduite afin d'identifier si la SSI est « **une bonne idée** ».

3.4.2. Seconde étape : comment gérer le risque SI

Cette étape consiste à s'informer sur l'innovation pour l'interpréter avant de mettre en perspective ses implications (Karahanna et al. 1999). Particulièrement à la SSI, il s'agirait, pour le potentiel adoptant, de comprendre comment la gestion du risque peut empêcher la survenance de risque SI et les concepts sécurité qu'il faut mettre en œuvre afin d'éviter les conséquences défavorables. Si une définition de la sécurité de l'information consiste à protéger les informations et les éléments critiques organisationnels, fonctionnels et techniques qui la supportent (Whitman et Mattord 2009 p. 8), alors les informations évaluées à cette étape du processus doivent porter sur l'ensemble de ces points.

Le cadre d'AS soulève la notion d'incertitude quant à l'innovation, liée au manque de connaissances sur celle-ci. Le potentiel adoptant prendrait alors des dispositions afin d'accroitre sa communication avec son environnement social. Les concepts sous-jacents à ses interactions seraient que la prise de connaissance relève directement de l'influence informationnelle et normative (Karahanna et al. 1999). Nous rappelons que deux influences majeures ont émergé de la littérature SSI et peuvent interagir : l'évaluation de la menace et l'évaluation de la réponse possible à cette menace (Liang et Xue 2009). Précisément, dans l'étape de renseignement, selon le modèle d'AS et les éléments identifiés dans la littérature SSI, s'il s'agit de recueillir des informations à la fois sur la menace et donc le risque, et sur la réponse possible à ce risque, la SSI en l'occurrence. S'il peut paraitre confus, à cette étape, d'acquérir des informations sur les deux aspects de la gestion du risque, menace et réponse, il pourrait s'agir d'introduire **une boucle de rétro-action dans le modèle d'AS**. En effet, nous pouvons aisément comprendre que le **processus d'AS ne se déroule pas de façon linéaire, mais, qu'inscrites dans le temps, les étapes se combinent entre elles**. Par

exemple, Williams et al. (2009), ont démontré les effets de la combinaison de pression coercitives, de pressions mimétiques et normatives internes et externes, sur l'adoption de mesures de sécurité de la chaine d'approvisionnement. Plus précisément, l'adoption de ces mesures a été réalisée sur une période de temps articulant les interactions et communications avec l'ensemble des acteurs de la chaine d'approvisionnement, qu'il s'agisse de partenaires commerciaux, de clients, d'institutions nationales ou encore de managers propres à l'organisation. Particulièrement aux influences internes pour l'adoption symbolique de la SSI, Hu et al. (2007) ont démontré que la maturité de la sécurité dans l'organisation reposait pour partie sur les apports mutuels entre top-managers et acteurs. Pour l'ensemble de ces raisons et en accord avec plusieurs auteurs en SSI (par exemple Dhillon et Backhouse 2001 ou Hu et al. 2007), nous postulons que la théorie néo-institutionnelle est adaptée pour expliquer comment des facteurs institutionnels, autant internes qu'externes, influencent le recueil de connaissance sur une idée ou concept « inconnu ». En effet, la théorie de l'isomorphisme institutionnel (Di Maggio et Powell 1983) montre que dans un même champ, parce que les organisations qui produisent des services ou des produits similaires, ou qui partagent des fournisseurs, des ressources ou des clients identiques, sont sujettes à des pressions institutionnelles, internes et externes, similaires, elles tendent vers une forme d'homogénéisation structurelle ou de standardisation pour renforcer leur légitimité.

3.4.3. Troisième étape : évaluer la SSI en regard du besoin

L'évaluation de la réponse au besoin est réalisée de façon abstraire dans la troisième étape de l'AS. Selon Karahanna et al. (1999) et Rawstorne et al. (1998) l'évaluation, dans cette étape de l'AS, repose sur des caractéristiques[57] telles que la complexité, la compatibilité et l'essayabilité. En regard de ce cadre, plusieurs commentaires, issus de la littérature SSI, peuvent être considérés par le potentiel adoptant lors de cette évaluation.

Selon Kankanhalli et al. (2003), souvent, les tops-managers manquent de connaissance des contres mesures possibles. Si ces connaissances sont acquises à l'étape précédente (recueil d'information), les moyens de protection possibles identifiés devront être projetés selon les caractéristiques spécifiques de l'organisation et de son SI, afin de répondre précisément au besoin (Hagen et al. 2008). En effet, d'une part, les top-managers ne sont pas toujours convaincus de l'efficacité des contre-mesures au risque (Kankanhalli et al. 2003). D'autre

[57] Sur les travaux de Fishbein et Ajzen (1975)

part l'investissement en ressources et les contraintes associées peuvent modifier l'évaluation de la solution (Kwon et Johnson 2014). En complément, les tops-managers ne sont pas toujours assurés de l'efficacité des mesures de sécurité, appuyant davantage sur l'inadaptation d'une réponse technique (Kankanhalli et al. 2003). Enfin, l'évolution des menaces, et donc des risques, pourrait laisser penser aux top-managers que la solution évaluée peut être efficace mais éphémère, relevant alors d'une décision conduisant à des investissements inutiles.

Ce commentaire est parfois prolongé jusqu'à évoquer que la SSI, relevant d'une réponse technique, ne permettra pas une réponse adaptée aux problématiques de l'organisation (Soomro et al. 2016). En ce sens, l'étape d'évaluation doit pouvoir éclairer le décideur sur un investissement opportun mais aussi de l'assurant d'une réponse adaptée, ce qui renforce la notion d'essayabilité, soit la possibilité d'un essai potentiel de la solution.

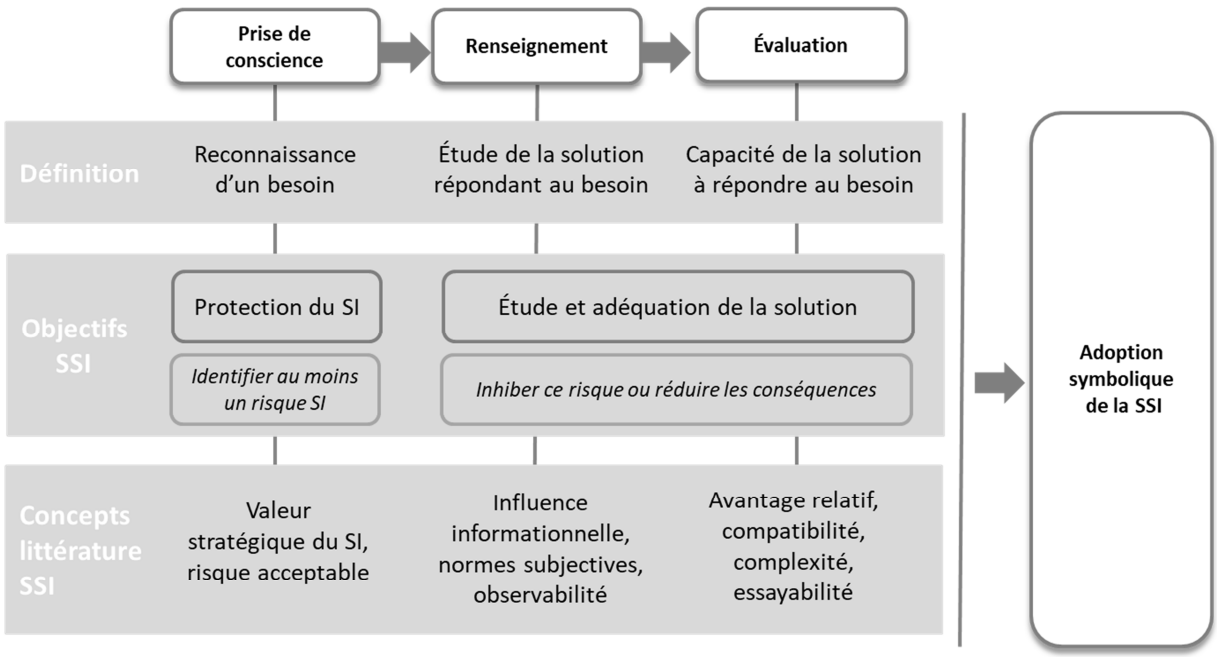


Figure 21 : Adaptation du modèle d'AS à la SSI

Le cadre d'AS adapté à la SSI ainsi défini offre un modèle théorique pour la décision d'adopter la SSI comme « bonne idée », en s'affranchissant des considérations liées à son développement « matériel ». L'étude des concepts qu'il mobilise devrait permettre d'appréhender s'ils sont activés et comment ils le sont lors du processus d'AS.

3.5. Conclusion du chapitre

Le chapitre précédent, traitant de sécurité des systèmes d'information, a mis en évidence que l'exposition accrue aux menaces pesant sur le SI relèverait d'une faible implication pour la SSI des top-managers, éclairant une posture réactive face aux risques (Goodhue et Straub 1991 ; Hu et al. 2007 ; Kankanhalli et al. 2003 ; Kwon et al. 2012). De nombreux auteurs relèvent que la décision d'organiser la protection globale du SI semble reposer sur les **risques perçus** (Albrechtsen et Hovden 2009 ; Slovic et al. 1979 ; Taylor 2006) ou les **risques vécus** (Choobineh et Dhillon 2007 ; Goodhue et Straub ; Kotulik et Clark 2004). Ainsi, la réflexion pour traiter ces risques SI peut émerger dès lors qu'un **incident effectif survient** (Kwon et al. 2012 ; Vance et al. 2014), soulignant la **faible perception des risques** SI des top-managers (Kankanhalli et al. 2003).

Dans cette perspective nous mobilisons un cadre théorique d'adoption symbolique afin d'étudier la décision d'adopter la SSI « immatérielle » qui serait alors une « bonne idée », sans considérations de la mise en œuvre effective qu'elles soient techniques, financières ou d'aptitude. Après avoir développé les raisons pour lesquelles l'AS est adaptée à notre projet de recherche, notamment grâce à la distinction entre adoption immatérielle et matérielle, nous l'avons enrichi de concepts directement ou indirectement développés dans la littérature SSI et issus de théories de la psychologie du risque ou de la théorie néo-institutionnaliste. En effet, l'étude de ces champs académiques a permis de faire émerger une relation étroite entre SSI, décision, risque et perception.

Précisément, nous avons développé les trois étapes de l'AS de Klonglan et Coward (1970) que sont « conscience », « renseignement » et « évaluation », en regard de la SSI et de la gestion des risques.

L'étape de **« conscience »** consiste, pour l'adoption d'une innovation, à reconnaître un **besoin** (Lesca et al. 2015 p. 43) ou à acquérir la connaissance sur l'existence et le fonctionnement d'une innovation (Rogers 2003 ; Sapp et Korsching 2004). Si cette étape est le point de départ du processus d'AS (Klonglan et Coward 1970) alors elle se traduit dans la discipline SSI par la prise de conscience d'un **risque à évaluer**, soit la perception des risques ou la solution innovante elle-même, soit la SSI. Particulièrement à la perception des risques, cette étape pourrait recouvrir la découverte du risque au travers de ses concepts « premiers », soit l'incertitude, les conséquences et son acceptabilité, dont nous avons décrit les composantes. Précisément, ces concepts sont traités par le décideur selon les influences de la perception des risques telle que la dimension et construction sociale des risques,

complétées de l'affect pour la situation risquée. En effet, Slovic (2000) et Sjöberg et al. (2004) précisent que plusieurs facteurs psychologiques, sociaux, culturels, politiques et institutionnels conditionnent la perception des risques. Ainsi l'évaluation du risque repose sur plusieurs éléments liés à l'évaluateur dans une situation donnée. Par exemple l'évaluation du risque peut être influencée par plusieurs facteurs comme la volonté d'exposition au risque, l'affect pour la situation risquée, la connaissance et l'immédiateté du risque, la nature des conséquences, l'importance « imaginée » ou « donnée » des conséquences (Fischoff et al. 1978 ; Finucane et al. 2000 ; Slovic et Peters 2006), soulignant la subjectivité de l'évaluation.

L'étape de **« renseignement »** prolonge la découverte nécessaire pour appréhender un objet inconnu (Karahanna et al. 1999 ; Sapp et Korsching 2004). Il s'agit, pour le potentiel adoptant, de recueillir les informations sur l'innovation afin de lever les incertitudes liées à une option jusqu'alors inconnue. Cette étape conduit le potentiel adoptant à accroitre ses interactions avec son environnement social (Karahanna et al. 1999) et à l'observer dans une approche combinant d'une part la légitimité de la solution et d'autre part la légitimité de ceux qui l'ont déjà adopté. En ce sens, Sapp et Korsching (2004) évoquent des « réponses émotionnelles et affectives aux messages » et en accord avec Rawstorne et al. (1998) la « persuasion sociale » et les « croyances normatives perçues ». Particulièrement à la SSI, cette étape articulerait les risques en regard des options pour protéger le SI, nécessitant de renforcer sa connaissance à la fois sur le risque et sur la SSI.

Nous notons la similarité des caractéristiques des étapes de conscience et de renseignement avec le fondement de l'évaluation des risques, qui peuvent se synthétiser dans les commentaires de Fischhoff et al. (1978) et de Slovic et al. (1980) : ce qui est en dehors de la vue est en dehors de l'esprit, suggérant que les risques doivent être perçus avant d'être traités. Ainsi, si la littérature SSI s'accorde sur la relation étroite entre protection du SI et gestion des risques, nous avons mis en évidence la nécessité de considérer les risques pour que la SSI soit un besoin identifié avant de l'adopter. En effet, il s'agit de s'intéresser à la SSI pour répondre à un besoin identifié, soit répondre à un risque pour Straub et Welke (1998) ou, à une exigence externe pour Hu et al. (2007).

Enfin, l'étape d'**« évaluation »**, consiste à évaluer l'adoption de l'innovation en l'appliquant de façon abstraite à la situation particulière du potentiel adoptant et aux spécificités de ses besoins (Klonglan et Coward 1970 p. 79). Elle fait interagir des caractéristiques telles que complexité, la compatibilité et l'essayabilité de la SSI (Karahanna et al. 1999 et Rawstorne et al. 1998). Si cette simulation nécessite d'identifier si la SSI permettrait de couvrir les risques

identifiés à la première étape plusieurs réserves émergent. D'une part, la complexité et l'abstraction des risques (Gerber et Solms 2005 ; Tsohou 2006) peut rendre cet exercice difficile. D'autre part ces contre-mesures technique et organisationnelle peuvent interroger le potentiel décideur sur l'efficacité de leur adaptation à leur propre situation (Kankanhalli et al. 2003 ; Kwon et Johnson 2014).

L'adoption symbolique, adaptée à la SSI distingue alors la première phase de l'adoption, en concentrant la perspective sur les éléments pris en compte avant la mise en œuvre pratique, permettant d'écarter alors des considérations qui pourraient masquer les influences sur la décision immatérielle.

Rappelons que, d'une part, la SSI est admise comme discipline de la gestion des risques (Goodhue et Straub 1991 ; Hu et al. 2007 ; Solms et Solms 2006a) positionnant la perception des risques, comme **première étape de la décision** dans les disciplines psychologique et SI (Fischhoff et al. 1978 ; Slovic et al. 1980 ; Straub et Welke 1998). Dans cette perceptive, il apparait pertinent de mobiliser ces disciplines pour notre étude. Par exemple, les facteurs culturels et organisationnels sont, selon Douglas et Wildavsky (1982) et parmi d'autres facteurs, importants pour comprendre le comportement à risque. Ainsi l'étude des risques sociétaux, producteurs d'incertitudes, peuvent éclairer les caractéristiques d'une société de risque. Particulièrement aux SI, les caractéristiques peuvent être comparables en regard de l'incertitude, des conséquences, et des mécanismes conduisant à un risque acceptable.

D'autre part, la gestion des risques s'inscrit comme une « décision comportementale » (Slovic et al. 1984 p. 183), visant, *in fine* à l'acceptation des risques selon les caractéristiques de celui-ci et des options de traitement choisies, déclinée par des mesurées de sécurité (Yates et Stone 1992). En ce sens, rappelons notre intérêt pour la décision d'engagement des dirigeants pour la SSI (Bandyopadhyay et al. 1999 ; Knapp et al. 2006 ; McFadzean et al. 2007), qui ne seraient pas toujours actée (Barlette et Fomin 2010 ; Johnston et Warkentin 2010 ; Straub et Welke 1998), notamment par une sous-estimation des risques SI (Albrechtsen et Hovden 2009 ; Choobineh et Dhillon 2007 ; Goodhue et Straub 1991 ; Kotulik et Clark 2004).

En ce sens, le cadre théorique mobilisé peut permettre de rendre intelligible les influences et leurs interactions sur la décision pour la SSI. Combinant les caractéristiques idiosyncratiques pour la perception du risque et les influences externes à l'individu, il peut éclairer la décision sur l'acceptation du risque et plus globalement sur l'adoption de la SSI,

dans la perspective des concepts d'auteurs en SSI (tel que Straub et Welke 1998 ou Liang et Xue 2009) et en gestion du risque sociétal (tel que Fischhoff et al. 1978, Slovic et al. 1980 ou encore Kermisch 2010, 2012).

Chapitre 4. Épistémologie et choix méthodologiques

« Depuis trois siècles, la connaissance scientifique ne fait que prouver ses vertus de vérification et de découverte par rapport à tous autres modes de connaissance. […] Et pourtant, cette science élucidante, enrichissante, conquérante, triomphante, nous pose de plus en plus de graves problèmes qui ont trait à la connaissance qu'elle produit, à l'action qu'elle détermine, à la société qu'elle transforme. » (Edgar Morin, Science avec conscience, 1982)

Toute recherche en gestion présuppose de questionner, de sélectionner et de décrire sa « démarche ». Si l'objectif de la recherche est de générer des connaissances « valables », il est nécessaire d'en préciser les justifications, classiquement à travers les questions épistémique, méthodologique et éthique (Avenier 2011 ; Le Moigne 2012), caractérisant le cadre épistémologique et aussi le rôle du chercheur dans le processus de production des connaissances scientifiques. Il s'agit de se positionner autour de trois questions. La question *gnoséologique* de la nature de la connaissance (le **quoi** ?), la question méthodologique traite de la *constitution des connaissances* (le **comment** ?) et la *question éthique* justifie la validité des connaissances (le **pourquoi** ?).

Avant de développer notre réflexion autour de ces trois questions, soulignons le propos de Le Moigne sur la finalité de ces questionnements, et du « contrat social » de nos travaux. Il nous apparait nécessaire, sinon inévitable, d'exposer en préambule le contexte dans lequel notre problématique a été initiée, soit l'origine de notre projet de recherche et de sa possible articulation avec les travaux académiques existants.

En tant que **praticien en SSI**, nous avons observé dans plusieurs entreprises les difficultés des managers intermédiaires à appréhender la protection du SI. Précisément, un engagement « minimal » de leur part pour cette problématique et la volonté de l'occulter auprès de leur direction posent naturellement la question « pourquoi ces pratiques » ? Pourquoi la SSI n'est pas mise en avant, pourquoi une discipline permettant d'assurer le fonctionnement du SI et par projection, les processus métier qu'il supporte, est considérée comme un sujet délicat qu'il faut traiter par nécessité lorsque des incidents surviennent et autrement pourquoi laisser aux seuls spécialistes techniques le soin d'empiler les solutions technologiques tout en limitant ces investissements « matériels ». Si la littérature académique offre une variété de raisons possibles à la deuxième partie du constat, telle

qu'exposé dans le chapitre « État de l'art de la sécurité des SI (p. 26), la première suscite davantage de questionnements. En effet, intuitivement, nous pensons que les conséquences défavorables possibles d'un défaut de protection relève du plus haut niveau de responsabilités, ne serait-ce qu'en considérant l'impact sur l'organisation. En effet, le CLUSSIF[58] suggère la perte possible de l'entreprise lorsqu'un sinistre majeur a impacté le SI (une étude conduite en 2006 montre que 2/3 des entreprises font faillite dans les 2 ans qui suivent un sinistre sur leur SI). Ainsi il s'agissait d'identifier le niveau de risque et les conséquences considérés par les « top-managers » de ces entreprises et d'observer les réponses qui y étaient apportées. Ensuite, si l'identification des risques est suggérée être le point initial pour la SSI (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Choobineh et Dhillon 2007 ; Kotulik et Clark 2004 ; Mitchell 1995), à notre connaissance la **littérature** est plutôt silencieuse sur les études exposant la prise en compte des risques pour la SSI par les top-managers. En ce sens, notons que la littérature appelle à investiguer la participation et l'engagement des décideurs stratégiques, que nous avons nommés « top-managers » (Crossler et al. 2013 ; Soomro et al. 2016 ; Tsohou et al. 2006). D'autres auteurs pointent la réactivité de la SSI, qui nécessite pour l'organisation de rencontrer un sinistre majeur avant que ne soit décidé la mise en œuvre de mesures de protection (Barlette 2012 ; Choobineh et Dhillon 2007 ; Goodhue et Straub 1991 ; Hagen et al. 2008 ; Kotulik et Clark 2004 ; Vance et al. 2014) renvoyant à des interrogations sur la perception et l'acceptation des risques. Enfin, la question des croyances des top-managers pour la SSI (Albrechtsen et Hovden 2009 ; Hu et al. 2007) semble que peu résolue.

À la lumière de la littérature et de plusieurs séances de travail avec d'autres chercheurs [59]en SI, le projet semblait, à ce moment-là, trop large car il associait décision des top-managers et mise en œuvre opérationnelle, ce qui soulevait finalement trois problématiques : 1) quelle décision pour la SSI et pourquoi, 2) quelles mesures sont effectivement mises en œuvre et pourquoi, 3) est-ce que la mise en œuvre correspond à la décision et pour quelles raisons ? En complément, s'il apparait évident d'investiguer le niveau organisationnel pour la question 2, il aurait sans doute fallu s'intéresser à l'individu « décideur » et son organisation dans le même temps pour les questions 1 et 3. Notre projet de recherche recentré et repensé vise alors à **rendre intelligible les influences prises en compte par les « top-managers » des entreprises pour protéger le SI, sans considérer la déclinaison opérationnelle de**

[58] Club de la Sécurité de l'Information Français

[59] Dont le 23ème Tutorat Doctoral Grand Sud à l'IAE d'Annecy en octobre 2016 et surtout un retour très constructif sur nos travaux par Suzanne Rivard qui les a alors qualifiés, en décembre 2016 de « projet d'une vie… ».

la SSI. Notre projet s'est ainsi construit sur la base d'un questionnement empirique, précisément un problème concret au sens de Thiétart et al. (2003 p. 49), puis confronté à la « connaissance académique », consistant à la volonté de comprendre les raisons prises en compte par les « acteurs décideurs » des organisations lorsqu'ils s'engagent pour la SSI.

Nous exposons l'épistémologie comme cadre mobilisé parmi les deux grands courants épistémologiques (Avenier et Perret 2012), pour **expliquer la / notre réalité**. La définition de l'épistémologie de Piaget (1967) permet de distinguer l'étude de la constitution des connaissances « valables », soit l'épistémologie, de l'étude de la constitution des connaissances soit la démarche de recherche, que nous développons en regard de notre projet dans la partie suivante.

4.1. Épistémologie

Le discours (logos) sur la connaissance (épistémè) appelle le chercheur à s'interroger sur « la légitimité des connaissances auxquels il fait appel pour élaborer en raisonnant ses comportement cognitifs et sociaux » (Le Moigne 2012 p. 3-4). Pour Gavard-Perret et al. (2008 p. 26), présenter les hypothèses fondatrices de son paradigme épistémologique est « un acte fondateur et fondamental qui a des conséquences sur toute la suite et notamment sur la validation/légitimation des résultats de sa recherche ». Il s'agit alors pour le chercheur d'expliciter les principes et les méthodes mobilisés dans ses travaux afin de les partager avec « sa » communauté (Kuhn 1962), en établissant un système cohérent de propositions et d'hypothèses fondatrices relatives aux questions épistémologiques. Précisément, pour Kuhn (1962 p. 10) « la ''science normale'' signifie la recherche fermement ancrée sur une ou plusieurs avancées scientifiques majeures passés, avancées qu'une certaine communauté scientifique particulière reconnaît, pour un temps, comme un apport aux fondations de sa future pratique ». Ainsi, lorsqu'on reprend la définition de l'épistémologie de Piaget (1967) ces hypothèses concernent la conception de la connaissance (hypothèses d'ordre épistémique), l'élaboration de la connaissance (hypothèses d'ordre méthodologique) et enfin la façon dont elle est justifiée (hypothèses d'ordre éthique). La plupart des paradigmes épistémologiques postulent préalablement des hypothèses d'ordre ontologique qui concernent le réel existentiel.

Si la consultation des ouvrages spécialisés rend compte d'une pluralité de paradigmes épistémologiques, en accord avec l'approche de Gavard-Perret et al. (2008 p. 20), nous nous attacherons à présenter celles qui « reçoivent un certain assentiment et une reconnaissance de la part des chercheurs en science de gestion » soit le paradigme positiviste et les paradigmes constructivistes. Ainsi, avant de justifier nos choix épistémologiques, nous dressons les hypothèses fondatrices de ces deux paradigmes dont nous discutons les caractéristiques et les principes.

	P.E. réaliste scientifique (Hunt, 1990, 1991, 1992, 1994, 2008 ; Bunge, 1993)	**P.E. réaliste critique* (PERC)** (Bhaskar, 1988)	**P.E. constructiviste pragmatique (PECP)** (von Glasersfeld, 1988, 2001 ; Le Moigne, 1995, 2001)	**P.E. interprétativiste** (Heidegger, 1962 ; Sandberg, 2005 ; Yanow, 2006)	**P.E. constructiviste au sens de Guba et Lincoln (PECGL)** (Guba et Lincoln, 1989, 1998)
Hypothèses d'ordre ontologique	Il existe un réel en soi (LE réel) indépendant de ce qui est perçu et des représentations qu'on peut en avoir.	Il existe un réel en soi indépendant de, et antérieur à, l'attention que peut lui porter un humain qui l'observe. Le réel est organisé en trois domaines stratifiés : le réel profond, le réel actualisé et le réel empirique.	Aucune hypothèse fondatrice. Il existe des flux d'expériences humaines	L'activité humaine est structurée (*patterned*). La signification consensuellement attribuée par des sujets à une situation à laquelle ils participent est considérée comme la réalité objective de cette situation.	Le réel est relatif : il existe de multiples réalités socialement construites, qui ne sont pas gouvernées par des lois naturelles, causales ou d'autre sorte.
Hypothèses d'ordre épistémique	LE réel (en soi) n'est pas forcément connaissable (faillibilité possible des dispositifs de mesure).	Le réel profond n'est pas observable. L'explication scientifique consiste à imaginer le fonctionnement des mécanismes générateurs (MG) qui sont à l'origine des événements perçus.	Est connaissable l'expérience humaine active. Dans le processus de connaissance, il y a interdépendance entre le sujet connaissant et ce qu'il étudie, lequel peut néanmoins exister indépendamment du chercheur qui l'étudie. L'intention de connaître influence l'expérience que l'on a de ce que l'on étudie.	Est connaissable l'expérience vécue. Dans le processus de connaissance, il y a interdépendance entre le sujet connaissant et ce qu'il étudie. L'intention du sujet connaissant influence son expérience vécue de ce qu'il étudie.	Dans le processus de connaissance, il y a interdépendance entre le sujet connaissant et ce qu'il étudie.
But de la connaissance	Connaître et expliquer des phénomènes observables (*via* éventuellement des concepts inobservables). Conception représentationnelle de la connaissance. Énoncés sous forme réfutable.	Mettre au jour les mécanismes générateurs et leurs modes d'activation. Conception représentationnelle des mécanismes générateurs.	Construire de l'intelligibilité dans le flux de l'expérience à fin d'action intentionnelle. Conception pragmatique de la connaissance.	Comprendre les processus d'interprétation, de construction de sens, de communication et d'engagement dans les situations. Conception pragmatique de la connaissance.	Comprendre les constructions de sens impliquées dans le phénomène étudié. Conception pragmatique de la connaissance.
Modes de justification spécifiques	Neutralité. Objectivité. Justification de la validité externe et de la validité interne (voir chapitres 2 et 3). Tests statistiques d'hypothèses. Réplication.	Pouvoir explicatif des MG identifiés. Justification de la validité des MG *via* des mises à l'épreuve successives dans des recherches quantitatives ou qualitatives.	Adaptation fonctionnelle et viabilité de la connaissance pour agir intentionnellement. Justification de la validité des connaissances génériques *via* des mises à l'épreuve dans l'action (recherches qualitatives).	Méthodes herméneutiques et ethnographiques. Justification des validités communicationnelle, pragmatique et transgressive.	Méthodes herméneutiques mobilisées de manière dialectique. Fiabilité (*trustworthiness*) et authenticité. Pas de généralisation.

* Au sens du réalisme critique transcendantal.

Figure 22 : Six paradigmes épistémologiques

(Avenier et Perret 2012 p. 25)

4.1.1. Positivisme

Selon Le Moigne (2012 p. 7) cette épistémologie institutionnelle fonde aujourd'hui « le tacite contrat social de la science et de la société », dominant les sciences de l'organisation depuis deux siècles, se revendiquant d'un positionnement réaliste, précisant qu'il s'agit pour son fondateur d'un terme désignant le « réel ».

Un fondement majeur de cette épistémologie relève de l'hypothèse ontologique qui postule l'existence d'un réel en soi et qui possède une nature propre. La connaissance relève alors de « la réalité essentielle de la réalité existentielle » (Le Moigne 2012). Il s'agit d'une réalité postulée indépendante des observateurs qui la décrivent, et qui sont des représentants « diplomatiques » de la connaissance observée, sans qu'elle ne soit représentée de façon parfaite. L'observation de l'objet réel par l'observant ne modifie ni l'objet réel ni l'observant, ce qui détermine, pour les positivistes, l'indépendance entre le sujet et l'objet de recherche (David 1999). En ce sens, pour Popper (1991 p. 185), « la connaissance, au sens objectif, est une connaissance sans connaisseur ; c'est une connaissance sans sujet connaissant ». L'observateur sait que la connaissance existe et tente d'établir la meilleure représentation, le plus proche possible (vérifiabilité) ou éloignée (falsifiabilité). Cette connaissance est conçue sur l'observation et l'expérience de faits sociaux, considérées comme des choses (Wacheux 1996 p. 39). Dans ce paradigme, les faits sont la base de la connaissance et seule l'observation permet de valider ou d'infirmer les construits. L'objectif est alors d'établir des régularités et des configurations de surface (Avenier et Thomas 2015), ou le plan de « câblage de l'univers » au sens de Le Moigne (2012) qui gouvernent les faits sociaux par l'observation de données d'expériences. La découverte des lois qui régissent les sociétés étant la finalité ultime de la science.

La deuxième hypothèse du positivisme relève justement de la « détermination naturelle » où chaque effet de la réalité est produit par quelques causes (Gavard-Perret et al. 2008 p. 22). Descartes décrivait une suite de raisons qui assurent que chaque effet est produit par quelque cause qui peut être identifiée « si l'on garde toujours l'ordre qu'il faut pour les déduire les unes des autres ». Autrement dit, le réel selon cette perspective est régi par les lois immuables de relations de causes à effet, observables et mesurables scientifiquement. L'hypothèse déterministe, aussi établie et enseignable soit elle, repose sur la croyance en la possibilité de décrire et d'expliquer la réalité dont on postule l'existence. Cependant les lois déterminant la réalité peuvent exister indépendamment de leur découverte (Le Moigne

2012). Selon cet auteur, « la croyance en l'hypothèse causaliste et donc en la possibilité non seulement de décrire, mais aussi d'expliquer de façon unique et permanente la réalité dont on postule l'existence » (Le Moigne 2012 p. 23).

Le paradigme épistémologique positiviste préconise deux principes méthodologiques le principe cartésien de division analytique et le principe de raison suffisante (Gavard-Perret 2008).

« Diviser pour régner » illustre le premier principe, ou selon Descartes, (Discours de la méthode) à, « […] diviser chacune des difficultés que j'examinerais en autant de parcelles qu'il se pourrait et qu'il serait requis pour mieux les résoudre ». Tel est le principe méthodologique, principe analytique d'Aristote, qui associe décomposition à réduction et ne permet alors pas d'observer les relations invisibles entre les éléments analysés (Le Moigne 2012 p. 26). Il implique que le réel connaissable soit décomposable en parties connaissables, reposant sur le précepte de Descartes qui assure que cette plus simple expression existe toujours, et qu'elle est facile à reconnaitre puisqu'elle se présente clairement et distinctement à notre esprit » (op. cit.)[60]

Le second principe est la « raison suffisante ». Établi par Leibniz[61] en 1710, le principe de raison suffisante assure que « l'existence d'un réel possible doit être expliquée syllogistiquement en raison » et selon les trois axiomes d'Aristote (raisonnement logique à deux propositions conduisant à une conclusion). Ce principe introduit la prégnance de l'approche déductive, « seule possibilité pour décrire la réalité ». Aisément et universellement enseignable, la logique déductive a été défendue par l'épistémologie institutionnelle » contre les paradoxes qui semble affecter (sa) cohérence ». Pour Thiétart et al. (2003 p. 22), « les positivistes, sur le postulat d'un déterminisme du monde social, visent à découvrir une **réalité extérieure** et les mécanismes qui la conditionnent. L'idéal positif serait d'atteindre la loi universelle expliquant la réalité, cette loi **révélant la vérité objective**. Même les plus classiques des positivistes reconnaissent que cet idéal reste une

[60] Notons ici le commentaire de Le Moigne (2012 p. 28) à l'endroit de la méthode de modélisation analytique : « Ce précepte de Descartes nous est bien peu d'utilité aussi longtemps qu'il ne nous dit pas comment décomposer en partie »

[61] Essai de théodicée, première partie, paragraphe 44, principe de la raison déterminante : «c'est que jamais rien n'arrive, sans qu'il y ait une cause ou du moins une raison déterminante, c'est-à-dire quelque chose qui puisse servir à rendre a priori, pourquoi cela est existant plutôt que de toute autre façon. Ce grand principe a lieu dans tous les événements, et on ne donnera jamais un exemple contraire : et quoique le plus souvent ces raisons déterminantes ne nous soient pas assez connues, nous ne laissons pas d'entrevoir qu'il y en a ».

utopie (Comte 1995) mais ils soutiennent que le chemin de la connaissance passe par l'appréhension des lois qui régissent la réalité ».

Selon Avenier et Gavard-Perret (2012 p. 18) il apparait à certaines communautés de chercheur « des domaines pour lesquels le modèle des sciences de la nature apparaît peu adapté ». Précisément dès que l'on considère « **la dimension humaine, le contexte, les interactions entre le chercheur et son sujet** », le modèle des sciences de la nature semble peu adapté difficile, « voire impossible » (Avenier et Gavard-Perret 2012 p. 19). En effet, notons le commentaire de Piaget (1967) pour qui la connaissance est un processus de construction de connaissances avant d'être un résultat et pour laquelle l'activité cognitive humaine **ne sépare pas aisément le connu et le connaissant**. Particulièrement l'action de connaître ne débute « ni par la connaissance du moi, ni par celle des choses comme telles, mais par celle de leur interaction ; c'est en s'orientant simultanément vers les deux pôles de cette interaction qu'elle organise le monde en s'organisant elle-même » (Piaget 1937, La construction du réel chez l'Enfant). En ce sens, évoqué une organisation « chemin faisant » de la connaissance nous évoque le poème d'Antonio Machado (1875 - 1939) :

Voyageur, le chemin
Ce sont les traces de tes pas
C'est tout ; voyageur,
Il n'y a pas de chemin,
Le chemin se fait en marchant…

4.1.2. Constructivismes

Différemment des sciences de la nature, les sciences de l'artificiel adressent les phénomènes qui ne relèvent pas seulement de la « Nature », mais offrent, sur la base de travaux de Simon (Avenier et Perret 2012) un modèle qui interroge comment les choses pourraient être faites, plutôt que sur les lois auxquelles elles devraient obéir (Le Moigne 2012). En ce sens, Thiétart et al. (2003 p. 19-20) indiquent que « la société possède une dimension artificielle objective. Et est construite grâce à une activité qui exprime un sens subjectif. C'est précisément le caractère dual de la société en termes d'artificialité objective et de signification subjective qui détermine sa « réalité *sui generis* ». Pour Avenier et Perret (2012 p. 20) l'artifice humain s'identifie dans « tous les éléments de notre environnement », ces éléments sont ceux que les

humains « construisent » tels que les produits, les services, les infrastructures ou encore les entreprises. Ainsi ces artefacts au sens de Simon, ont des propriétés spécifiques intrinsèques aux êtres humains qui ne sont pas « des objets inertes et passifs. », ce qui implique « un rôle crucial dans de nombreux phénomènes étudiés dans les sciences de gestion » (Avenier et Perret 2012 p. 20). En ce sens, Le Moigne (2012 p. 72) indique que le réel connaissable est un réel en activité qu'expérimente le sujet, rejoignant le commentaire de Piaget sur l'interaction pour la connaissance. Précisément, David (1999 p. 16) soutient que l'interaction entre artefacts et chercheur permet, à l'appui de l'expression de Koenig, « la maîtrise du monde », ou « du moins, une participation à sa construction et à son pilotage ».

Un exemple reconnu d'individus guidés par leurs finalités, par leurs interactions avec leur environnement, leurs pensées et leurs actions, est énoncé par Watzlawick (1988) dans le cas des prophéties auto réalisatrices. La prophétie auto réalisatrice est une supposition qui, par le simple fait d'avoir énoncée, entraine la réalisation de l'évènement prévu et confirme ainsi son exactitude. Selon Watzlawick (1988 p. 109), « la prévisibilité du comportement ne serait pas liée à un déterminisme en dehors des acteurs mais à la soumission des acteurs à un emprisonnement dans un jeu sans fin qu'ils ont eux-mêmes créé ».

Selon Avenier et Perret (2012 p. 21), pour la science de l'artificiel, « la recherche vise à développer des connaissances relatives au fonctionnement et à l'évolution d'artefacts dans leur contexte » en s'appuyant sur la proximité entre science de l'artificiel et « science d'ingénierie » suggérée par Simon. Ainsi, les sciences de gestion sont définies comme une science de l'action, où l'intervention en gestion est considérée comme un **projet d'action**. L'action, au sens de Le Moigne (2012 p. 72), porte à la fois sur le « faire », soit le mode d'élaboration de la connaissance et sur la « connaissance de l'objet » dans laquelle il s'agit bien de conception intentionnelle dans la perspective d'un projet d'action. Cela rejoint le propos de David (1999 p. 13) qui souligne que « les sciences de gestion auraient donc vocation à analyser et à concevoir les dispositifs de pilotage de l'action organisée ».

	Positivisme	**Constructivisme**
Hypothèse épistémologique et vision de la réalité	Réaliste Ontologie du réel	Relativiste Phénoménologie du réel
Objectif de la recherche	Identifier des régularités et des configurations de surface	Construire des modèles intelligibles de l'expérience humaine
Nature de l'objet de recherche	Interrogation des faits	Développement d'un projet

		de connaissance
Nature, origine et validité de la connaissance produite	Objective et acontextuelle Observation de la réalité Cohérence avec les faits	Subjective et contextuelle Construction Convenance pour le projet
Nature du lien sujet / objet	Indépendance Sujet -> Objet cible	Interaction Sujet <-> Objet cible
Vision du monde social	Déterminée	Intentionnelle

Tableau 8 : Synoptique des hypothèses et principes du positivisme et constructivisme

(adapté de Thiétart et al. 2003, Avenier et Thomas 2015 et al. 2006 p. 213)

Le constructivisme permet ainsi une attitude ouverte de recherche, plutôt qu'un paradigme définitif (Wacheux 1996), dont le dénominateur commun est une manière de se comporter et de penser. Ainsi, si David (1999 p. 10) relève non pas un paradigme constructiviste mais plutôt une « école » regroupant « un ensemble d'approches très variées » nous nous attacherons à présenter les deux constructivismes essentiels en science de gestion (Gavard-Perret et al. 2008 p. 24). Le paradigme conceptualisé par Guba et Lincoln et le paradigme développé par Piaget, Von Glasersfeld et Le Moigne, nommé pragmatique, convergent par leur hypothèse épistémique et diffèrent par leurs positions ontologiques et par leur méthodologie.

Pour le **paradigme constructiviste pragmatique**, la **première hypothèse** postule que ce qui est connaissable est l'expérience d'UN réel. Précisément, pour Le Moigne (2012) « le réel connaissable est un réel en activité qu'expérimente le sujet ». Ainsi, Gavard-Perret et al. 2008 p. 35) citant Von Glasersfeld[62], précise que le constructivisme est radical car ce qui est connaissable relève exclusivement de « la mise en ordre et l'organisation d'un monde constitué par notre expérience » et non pas d'une réalité ontologique ''objective'' ». Ce commentaire permet de souligner que la première hypothèse est fondée sur un réel connaissable dépendant des perceptions qu'il induit. Cette absence d'hypothèse fondatrice

[62] (Von Glasersfeld 1988 p. 27)

sur la nature de la réalité « rend possible pour un chercheur » de « poser des hypothèses de travail d'ordre ontologique concernant le réel étudié[63] » Avenier et Perret 2012 p. 36)

La **deuxième hypothèse** relève de l'interdépendance du sujet et de l'objet. Selon Gavard-Perret et al. (2012 p. 36), « ce qui relève uniquement du réel étudié est inextricablement tissé avec ce qui relève du sujet connaissant ». Pour Le Moigne (2012 p. 75) la « récursivité de la cognition » s'agit justement de l'interdépendance entre le phénomène perçu et la connaissance construite ; citant Theodosius Dobzhansky (1900-1975), « en changeant ce qu'il connait du monde, l'homme change le monde qu'il connaît ».

La **troisième hypothèse** du paradigme constructiviste**,** dite **téléologique,** postule que le projet de connaitre un certain réel influence la manière dont on en fait l'expérience, et donc la connaissance que l'on en développe. Le Moigne (2012) précise que « connaitre en termes de fins plausibles constitue un mode de **connaissance légitime** surtout si rien n'assure que le phénomène considéré à une cause certaine et que ce phénomène peut avoir de multiples fins ''déterminées à chaque instant de façon **endogène**'' ». Thiétart et al. (2003 p. 44) rappellent que la construction d'un chercheur dans une approche constructiviste est établie « à partir et d'après sa propre expérience, dans le contexte d'activation qui est le sien », renvoyant alors au concept de développement d'un projet de connaissance. Selon nous, un exemple illustrant cette hypothèse est celui de l'analogie de la clé et de la serrure. Von Glasersfeld (1988 p. 34) indique que si « l'activité humaine de connaître ne mène jamais à une image du monde qui soit certaine et vraie, mais seulement à une interprétation conjecturale, alors on peut comparer cette activité avec la fabrication de clés dont l'homme se sert pour ouvrir des voies vers les buts qu'il choisit d'atteindre. (…). En effet, l'efficacité d'une clé ne dépend pas du fait de trouver une serrure à laquelle elle convienne : la clé doit seulement ouvrir le chemin qui mène au but précis que nous voulons atteindre ».

Ces connaissances sont alors construites comme UNE représentation des traits essentiels d'une réalité et sont modélisées sous forme de représentation offrant des « repères viables pour agir intentionnellement par rapport au phénomène étudiés » (Gavart-Perret et al. 2012 p. 36). Puisque nous accédons aux connaissances par les représentations que nous en construisons et que nous les représentons par des systèmes de symboles, il 'agit alors de

[63] Avenier et Perret (2012 p. 61) précisent que « dans un projet de recherche, une hypothèse de travail est une hypothèse postulée dans le cadre du projet considéré et que ce projet ne vise pas à questionner »

modéliser des artefacts. Ainsi le terme modélisation prend tout son sens dès lors qu'il s'agit, pour le chercheur, de donner une représentation d'un phénomène dans son contexte. Comme le souligne Gavard-Perret et al. (2012), il s'agit moins de présenter une représentation de régularités du réel mais davantage d'en développer une compréhension des raisons plausibles.

Pour le **paradigme constructiviste conceptualisé par Guba et Lincoln**, si les hypothèses d'ordre épistémique et téléologique sont proches, c'est sur la première hypothèse, ontologique, que les deux constructivismes divergent. Effet, si le pragmatisme postule ne postule aucune hypothèse fondatrice d'ordre ontologique et se rattache au pragmatisme, le constructiviste conceptualisé par Guba et Lincoln conçoivent une hypothèse relativiste qui stipule le caractère relatif de ce qui existe (Avenier 2011). « Cette réalité relative et multiple consiste en des significations individuelles conçues par des individus dans une tentative de donner du sens aux expériences qu'ils vivent ». Il s'agit alors pour le chercheur de faire émerger des significations des interactions.

En synthèse des différences entre le paradigme Constructiviste conceptualisé par Guba et Lincoln et le paradigme constructiviste pragmatique, le tableau 9 en présente un synoptique complété des hypothèses méthodologiques développées ci-après.

Paradigme Épistémologique	**Constructiviste**	**Pragmatique**
Hypothèses fondatrices		
Nature de la connaissance	***Hypothèse d'ontologie relativiste :*** Il existe de multiples réalités socialement construites, qui ne sont pas gouvernées par des lois naturelles, causales ou d'autre sorte.	***Hypothèse de connaissance phénoménologique :*** L'existence d'*un réel tel qu'il peut être en lui-même* n'est pas niée a priori, mais aucune hypothèse fondatrice n'est postulée sur l'existence et la nature d'un *réel en soi*. La confrontation des connaissances que différents humains ont d'un phénomène ne permet pas de garantir l'élaboration d'une connaissance objective d'*un (possible) réel en soi*, qui serait indépendante des sujets connaissant et de leurs contextes d'étude.
But de la connaissance	Comprendre comment des	Construire des **modèles**

	individus **donnent du sens** aux expériences qu'ils vivent	**intelligibles de l'expérience** humaine, offrant des repères **adaptés** et **viables** pour organiser le monde de l'expérience.
Hypothèses méthodologiques	Seules les méthodes herméneutiques et dialectiques, mises en œuvre de manière éthique, sont éligibles. Critères d'évaluation de la qualité d'une recherche : crédibilité, authenticité.	Toute méthode, y compris les méthodes herméneutiques et dialectiques sont éligibles. Principes directeurs : comportement éthique, explicitation des hypothèses et du processus d'élaboration des connaissances, et rigueur critique dans la conduite de ce processus.

Tableau 9 : Synoptique des hypothèses et principes des constructivismes

(adapté de Avenier 2011 et Avenier et Thomas 2015)

Le paradigme épistémologique constructiviste préconise deux principes méthodologiques, la modélisation systémique et le principe d'action intelligente.

Selon Le Moigne (2012 p. 94), la modélisation ou médiation d'un objet porte sur « l'acte et non sur la chose », la question posée est « qu'est-ce qu'elle fait et pourquoi ? ». La modélisation fait état de la complexité et les sens qu'elle peut attribuer à l'objet en préservant l'objet « ouvert» et ne « cherchant pas l'exhaustivité », en opposition aux épistémologies cartésiano-positivistes. Plutôt que de simplifier pour rendre plus facilement présentable, il est préférable de modéliser pour rendre intelligible. La modélisation relève alors d'un processus d'élaboration des connaissances, elles-mêmes entendues comme processus cognitif autant que comme résultat sous forme de représentation désignées. Les connaissances ainsi construites sont des connaissances comme les « autres » accessibles comme elles par des systèmes de symboles souvent perçus complexes mais intelligibles par l'esprit humain qui les élabore et qui les considère. Ce principe est établi sur les bases de :

- Montaigne et Pascal : « toutes choses étant causées et causantes, aidées et aidantes, médiates et immédiates, et toutes s'entretenant par un lien naturel et insensible qui lie les plus éloignées et les plus différentes, je tiens impossible de connaître les parties sans connaître le tout, non plus que de connaître le tout sans connaître partiellement les parties » et,
- Vico et Léonard de Vinci : l'ingénium s'attache à décrire la situation dans son contexte, description qui repose sur la capacité des individus à raisonner faculté en reliant de manière rapide, appropriée et heureuse des choses séparées.

Le principe d'action intelligente caractérise la « capacité d'un système cognitif explorant et construisant les représentations symboliques des connaissances ». Contrairement à l'exigence de connaissance « vraie », ce principe utilise les ressources du raisonnement dialogique dès lors qu'elles sont reproductibles. Les connaissances du modélisateur sont argumentées et non démontrées car elles reposent sur la construction par celui-ci. Ainsi, selon (Le Moigne 2012 p. 95) ce mode de connaissance fonctionnelle s'avère pragmatiquement producteur d'intelligibilité car il permet de comprendre en construisant **une signification à la fois stable** (basée sur des hypothèses plausibles et i**nterprétable** comme telle par le sujet connaissant : il **connait ce que ça fait ou peut faire**, s'il ne connait pas encore de quoi c'est fait (connaissance organique), et il sait interpréter ces fonctions en référence à quelque projet (connaissance projective). Ce principe émane de Vico qui précise que « le vrai et le faire sont une seule et même chose » (théorie du verum factum).

Pour Avenir (2011 p. 384) ces deux paradigmes ne prétendent pas l'accès à un fonctionnement réel d'un artefact mais davantage à en élaborer une représentation « congruentes ». Si ces représentations sont modélisées par des individus « concernés par la situation » dans un contexte donné, l'évaluation des connaissances diffèrent dans ces deux paradigmes.

Pour le constructiviste conceptualisé par Guba et Lincoln, la co-construction d'individus aboutit à un consensus sur le phénomène considéré. Cette signification partagée la plus représentative implique alors qu'il n'y en a pas d'autre pour ces individus. Ce consensus apparait moins clairement dans le pragmatisme attendu que le sujet connaissant représente l'expérience de l'individu considéré. Précisément, l'évaluation « des connaissances repose sur la confrontation à l'expérience de l'action » (Avenier 2011 p. 384) ce qui ne permet pas un accord et consentement explicite de l'individu.

4.1.3. Posture épistémologique constructiviste pragmatique

Notre projet de recherche vise à construire des connaissances théoriques et des connaissances actionnables, c'est-à-dire d'en produire une connaissance enseignable qui favorise l'émergence de représentations nouvelles pour la SSI. Précisément il s'agit de rendre intelligible les influences prises en compte par les « top-managers » et conduisant à

l'adoption symbolique de la sécurité des systèmes d'information, sans expliquer les raisons de leur interaction ou du résultat. En accord avec Charreire et Huault (2001), se prévaloir d'un paradigme épistémologique constructiviste par la nature même des objets étudiés est insuffisant. Nous souscrivons alors à la recommandation de David (1999) qui consiste à justifier la cohérence entre processus de recherche spécifiques mobilisés et les résultats, avec les hypothèses fondatrices de ce paradigme.

En regard de l'exposé des paradigmes positiviste et constructivistes, en cohérence avec nos objectifs de recherche, et dans la perspective de la finalité de notre projet, nous adoptons le constructivisme pragmatique, tel qu'explicité par Le Moigne (2012), comme posture épistémologique pour notre travail doctoral. Nous justifions notre positionnement épistémologique au travers des réponses aux questions **d'ordre épistémique**, **méthodologique** et **éthique**. Ces trois questions ont des implications concrètes et réelles pour notre recherche dans la mesure où elles demandent à « réfléchir à la pertinence et à la validité du processus d'élaboration des connaissances mis en œuvre au regard de l'objectif poursuivi » qui reste la finalité d'un projet de recherche (Avenier et Gavard-Perret 2012 p. 13).

L'hypothèse fondatrice du paradigme constructiviste pragmatique indique que de **l'expérience humaine est modélisable**, la confrontation des connaissances que différents humains ont d'un phénomène ne permet pas de garantir « l'élaboration d'une connaissance objective, d'un possible réel en soi » (Avenier 2011 p. 377). En effet, ce « réel » est expérimenté par le sujet connaissant, constitué « d'interprétations qui se construisent grâce aux interactions » (Charreire et Huault 2001 p. 32). En perspective de l'hypothèse d'interdépendance, cette expérience est influencée par les caractéristiques idiosyncratiques du sujet connaissant, telles que « les finalités de son projet de connaissance, le contexte dans lequel il se situe, ses valeurs, sa culture et plus généralement son histoire » (Avenier 2011 p. 385 ; Le Moigne 2012). Cette perspective correspond à la philosophie de notre projet, tant sur l'interdépendance avec notre expertise sur la gestion du risque que l'idée d'émergence de nouvelles connaissances par l'interaction avec des acteurs terrain.

Aussi, cette approche est en accord avec **l'hypothèse téléologique** que nous adoptons, soit construire un projet de connaissance d'un réel dont on en fait l'expérience pour en développer des connaissances (Le Moigne 2012). Rappelons que, pour cet auteur, l'hypothèse téléologique vise à considérer la finalité du sujet connaissant avec un principe de modélisation systémique en préférant s'intéresser à leurs missions et projets plutôt qu'à leur composition. Ainsi, selon Avenier et Perret (2012 p. 36), ces connaissances sont

exprimées sous la forme de constructions symboliques ou modélisations. Cela nécessite alors de montrer que ces connaissances sont « fonctionnellement adaptées à son expérience de la situation étudiée, et constituent pour les acteurs des repères viables pour intervenir intentionnellement au sein de cette situation » (Avenier et Perret 2012 p. 43). Nous adhérons au principe même d'artefact pour notre projet de recherche pour plusieurs raisons principales. Nous souhaitons rendre intelligible la nature des influences qui peuvent interagir dans la réflexion des individus lorsqu'il s'agit d'adopter symboliquement la SSI. Il s'agit alors, pour les individus, d'exprimer ces influences au moment où cette réflexion a été conduite. En l'absence de connaissances partagées sur ce sujet, seule la co-construction d'une réalité entre sujet connaissant et individu décideur (David 1999) peut permettre de dresser des représentations de son expérience, qui sont alors élaborées « grâce aux interactions » (Charreire et Huault 2001 p. 32).

Notons qu'Avenier (2011 p. 382) précise qu'adopter une posture épistémologique constructiviste pragmatique, en regard des hypothèses de travail d'ordre ontologique, offre la possibilité d'intégrer des savoirs qui ont été développés dans d'autres paradigmes épistémologiques ». En ce sens, ces propos rejoignent ceux de David (1999 p. 1) qui suggère de « dépasser l'opposition entre positivisme et constructivisme, dissiper certaines confusions, par exemple celles résultant d'associations trompeuses entre positivisme et méthodes quantitatives ou, de manière symétrique, entre constructivisme et méthodes qualitatives pour explorer les différentes implications d'une conception constructiviste en sciences de gestion ». Pour nos travaux, si la littérature en SI que nous mobilisons est issue de différents courants théoriques et d'épistémologies positiviste et constructiviste, les cadres théoriques d'adoption symbolique et la psychologie sociale s'inscrivent dans un courant déterministe. En considérant avec soin ces fondamentaux, nous soulignons d'une part que nous ne visons pas à éprouver le cadre d'adoption symbolique, les théories de perception du risque en psychologie sociale ou encore le néo-institutionnalisme. D'autre part, nous mobilisons ces travaux dans l'objectif d'« intégrer ces savoirs » en les réinterprétant pour notre projet (Avenier 2011 p. 382).

Ainsi, une fois exposé notre cadre épistémologique, nous pouvons aborder les modes de constitution de connaissance, en nous interrogeant sur les hypothèses fondamentales sur

lesquelles reposent notre conception de la connaissance afin de justifier le recours à une méthode qualitative.

4.2. Méthodologie

Avenier et Perret (2012 p. 14) rappelle que le questionnement épistémologique initial, « vise à clarifier la conception de la connaissance sur laquelle le travail de recherche reposera et la manière dont seront justifiées les connaissances qui seront élaborées. Ce travail épistémique permet ensuite d'élaborer la réflexion méthodologique, que nous présentons dans cette section.

Ainsi, après avoir posé les bases et justifié notre choix épistémologique, il s'agit de dresser « la trame qui permet d'articuler les différents éléments d'une recherche « problématique, littérature, données, analyse et résultats » (Thiétart et al. 2003 p. 139). Selon Miles et Huberman (2003 p. 38) les canevas de recherche « qualitatifs ne sont ni des modèles transposables ni des solutions miracle qui supprimeraient l'existence d'un travail analytique construit, révisé, chorégraphié ». Ainsi, en synthèse de notre travail analytique nous présentons une représentation de ce projet de recherche.

Nous présentons notre démarche de recherche en justifiant le choix de la méthode retenue, selon notre projet et le mode d'évaluation de la connaissance avant de présenter le matériel empirique et l'analyse des données.

Pour justifier nos choix méthodologiques, nous n'évoquerons pas l'opposition souvent rencontrée entre méthode quantitative et qualitative. Notre vision est plus proche de David (1999 p. 2) qui, précisément, recommande de « dépasser l'opposition classique entre démarche inductive et démarche hypothéticodéductive et considérer une boucle récursive abduction/déduction/induction. », quand bien même « cette boucle n'a **pas besoin d'être parcourue intégralement par chaque chercheur ou au sein de chaque dispositif de recherche** ».

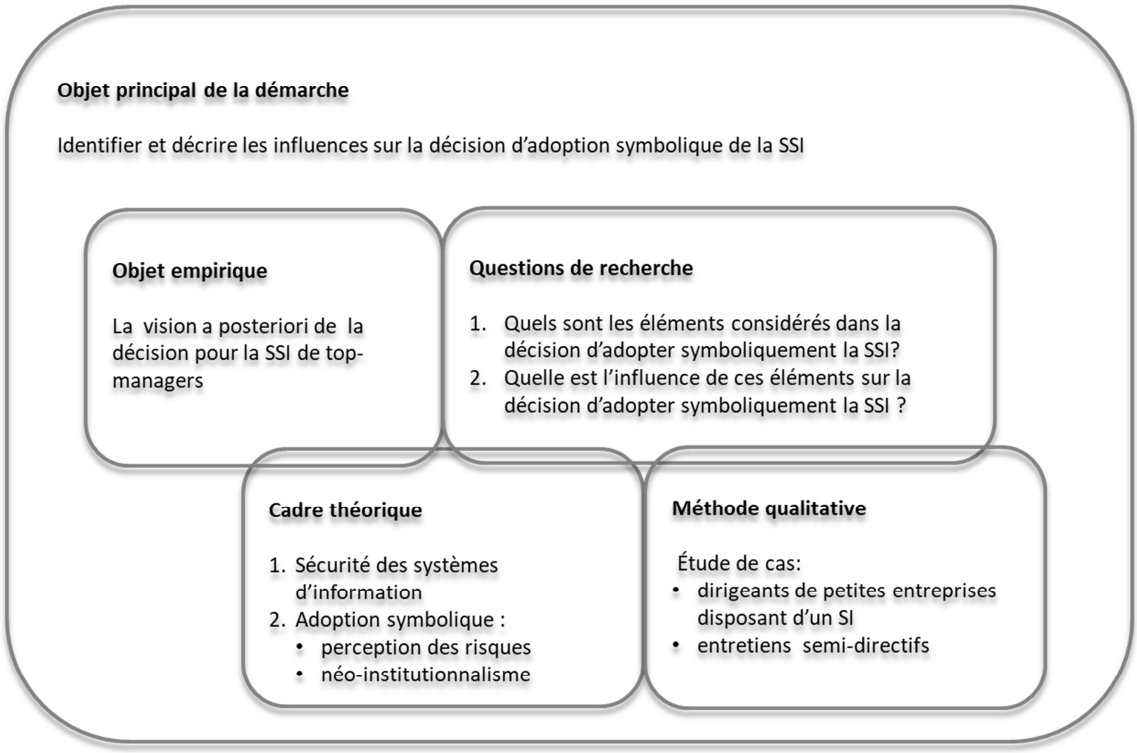


Figure 23 : Synthèse du design de recherche

Nous nous inscrivons aussi dans une recherche pour la science de l'artificiel au sens développé par Avenier et Perret (2012 p. 21) qui « vise à développer des connaissances relatives au fonctionnement et à l'évolution d'artefacts dans leur contexte ». En effet, notre objectif n'est pas d'expérimenter pour découvrir la « nature des choses en soi » mais d'évaluer l'adéquation d'une représentation avec l'expérience empirique (Von Glasersfeld 1988). Précisément nous souscrivons au commentaire de Le Moigne selon qui l'information vient se confondre avec la connaissance, et adoptons une approche systémique de l'information qui ne peut être considérée indépendamment de l'acteur, de son espace cognitif et du contexte de perception. Notre méthodologie est centrée sur la génération de connaissances actionnables selon un contrat social explicite et détaillé. Nous utilisons pour ce faire une méthode qualitative encadrant plusieurs études de cas avec plusieurs unités d'analyse telles que décrite dans la section ci-après.

4.2.1. Choix de la méthode qualitative

Le choix de la méthode qualitative a été effectué naturellement en regard **du paradigme épistémologique** dans lequel nous positionnons et **de notre projet**. L'objectif est d'utiliser

les connaissances produites par **l'étude de cas** pour construire des connaissances actionnables, à partir des contraintes réelles du terrain. Notre recherche s'inscrit dans une approche qualitative à visée exploratoire, descriptive et compréhensive. Une méthode qualitative organisée autour de plusieurs études de cas est alors apparue pertinente.

En effet, l'objectif de nos travaux est à visée exploratoire, compréhensive et descriptive. L'exploration sert deux objectifs principaux que sont la compréhension, d'une part, et l'explication d'autre part d'un phénomène complexe où les **concepts en jeu sont polymorphes**. Ainsi, nous ne projetons pas de rechercher des relations causales ou de prédire des phénomènes (Thiétart et al. 2003 p. 22). Nous aspirons à identifier et comprendre des phénomènes sociaux sous l'angle idiosyncratique et interactionniste entre le « décideur » et son environnement dans un contexte d'organisation et pour son système d'information dans son entreprise. En ce sens, rappelons que le choix cohérent d'une méthode devait s'inscrire dans la science de l'artificiel dans laquelle « la recherche vise à développer des connaissances relatives au fonctionnement et à l'évolution d'artefacts dans leur contexte » (Avenier et Perret 2012 p. 21). Plus généralement, ces mêmes auteurs notent que « les méthodes qualitatives reposant sur des interactions approfondies avec des acteurs organisationnels sont privilégiées dans les paradigmes épistémologiques autres que positivistes et post-positivistes », (op. cit. p. 43). Citant Bhaskar, Avenier et Perret (2012 p. 34) indiquent que les particularités des phénomènes sociaux induisent plusieurs conséquences méthodologiques importantes. « D'une part, étant difficiles à mesurer, les phénomènes sociaux peuvent seulement être compris, une spécificité qui plaide en faveur d'un recours aux méthodes qualitatives. » « D'autre part, les phénomènes sociaux se manifestent au sein de systèmes ouverts et ne peuvent pas être artificiellement clos au sein d'une expérimentation ». L'étude de cas se définit justement, selon Yin (1989 p. 17), « une recherche empirique qui examine un phénomène contemporain dans un contexte réel lorsque les frontières entre le phénomène et le contexte n'apparaissent pas clairement, et pour laquelle de multiples sources de données sont utilisées ». Cet auteur stipule que l'étude de cas est une voie privilégiée lorsque le chercheur souhaite répondre à des questionnements concernant le « comment ? » et le « pourquoi ? ». En d'autres termes, lorsque les problématiques sont axées sur la compréhension d'une situation, sa représentation, où l'analyse de processus complexes.

Ces études supposent un contact approfondit avec le terrain et l'accès à une richesse de données autorisant ainsi, une analyse fine. L'étude de cas qualitative nécessite « une bonne interaction entre données observées, acteurs étudiés et chercheur ». Elle met également

l'accent sur la compréhension des dynamiques présentes à l'intérieur d'un environnement unique et se limite à un domaine d'investigation bien spécifique (Yin 1989). Pour Miles et Huberman (2003 p. 55), un cas peut être défini comme « « un phénomène qui se produit dans un contexte délimité ». Dumez (2011 p. 56) soutient la justification d'un choix pour l'étude de cas par « une analyse fine, détaillée des phénomènes étudiés, incluant la description et la narration, présentant les acteurs et leurs actions et interactions, leurs discours et interprétations, et la mise en évidence de mécanismes sous-jacents aux dynamiques et processus ». Il détaille particulièrement, la visée compréhensive de la recherche et le champ d'investigation. La **visée compréhensive** de la recherche nécessite de déterminer l'unité d'analyse selon la question de recherche, les cadres théoriques mobilisés et les données rassemblées. Le choix de l'unité d'analyse conditionne le **champ d'investigation** que nous détaillons dans la section « entretiens » ci-après. Il précise que l'évolution de ce champ doit être « expliquée et justifiée » (Dumez 2011 p. 56).

Pour Thiétart et al. (2003) les méthodes qualitatives permettent de réaliser des entretiens, soit une technique destinée à collecter, dans la perspective de leur analyse, **des données discursives reflétant notamment l'univers mental conscient ou inconscient des individus** Notons les appels de plusieurs auteurs en SSI tels que Dhillon et Backhouse (2001 p. 133) ou encore Backhouse et Dhillon (1996) qui critiquent la forte mobilisation des approches « fonctionnalistes » et les conduisent à conclure que « le comportement, les intentions et les modèles comportementaux des gens ont en grande partie été ignorés » dans ces études. Ils proposent alors de viser « une compréhension qualitative de sécurité de l'information » peut être avantageuse grâce à de la capacité de faire des recherches sur le phénomène dans les limites de l'organisation (Dhillon et Backhouse 2001 ; Taylor 2006) »

Ensuite, en regard de notre projet et du peu de travaux académiques[64] sur les influences possibles sur la décision d'adopter symboliquement la SSI, nous souscrivons au commentaire de Gavard-Perret et al. (2012). Ces auteurs soulignent qu'une des distinctions liée aux recherches qualitatives est de comprendre en profondeur un phénomène, compréhension rendue possible par la richesse et la complexité des données qualitatives. Celle-ci permet notamment une vision globale holistique ou systémique, à même de prendre en comptes des interactions multiples et leur articulation avec un environnement particulier » (Gavard-Perret et al. 2012 p. 248). Cela rejoint alors les propos de Thiétart et al. (2003) qui précisent la dépendance fondamentale entre le processus d'élaboration de la connaissance et la nature

[64] Précisément huit à notre connaissance abordent la SSI sous l'angle de la décision (cf. 3.2.7 « Perception des risques et SSI » p. 161)

de l'objet de recherche. En effet, la dynamique projective caractéristique du processus de construction de la connaissance constructive se traduit méthodologiquement comme un processus de résolution de problème dont la mise en œuvre s'opère grâce à la formulation de représentation et /ou d'outils **nouveaux** (Thiétart et al. 2003 p. 45). Ainsi, comme le préconises (Avenier et Perret 2012 p. 14), il s'agit d'accéder au terrain afin de « comprendre le fonctionnement d'artefacts existants » et d'étudier « les processus mis en œuvre, les acteurs internes impliques, les principales parties prenantes externes, les projets respectifs et les attentes » des acteurs.

Enfin, traiter de SSI relève d'une double sensibilité. D'une part, il fait consensus que les informations sur la SSI sont considérées comme sensibles et souvent confidentielles (Kotulic et Clark 2004) donc peu communicables. D'autre part, nos travaux nécessitent d'identifier des influences liées à « l'environnement » du décideur mais également à ses caractéristiques personnelles telles que ses expériences, connaissances, objectifs, priorités, motivations, et valeurs et comportement, pouvant accentuer leur réticence à les communiquer.

Ainsi, notre stratégie de recherche s'inscrit dans l'étude de cas. Cette stratégie d'accès au réel est largement utilisée en sciences de gestion. Elle permet « de suivre ou de reconstruire les événements dans le temps (chronologique), d'évaluer les causalités locales [...] et de formuler une explication » (Wacheux 1996).

Afin de prolonger l'éclairage sur notre choix méthodologique, il s'inscrit en regard des limites et des particularités que présente la méthode qualitative, telles que synthétisées dans le tableau ci-après.

Les limites de la recherche qualitative	**Les prescriptions/particularités de la recherche qualitative**
– Le manque de fiabilité ; – Les objets étudiés sont complexes, comprennent de nombreuses variables et interrelations et sont fortement dépendant du chercheur ; – Les données recueillies et analysées sont liées au chercheur par leur choix et leur interprétation et sont considérées comme subjectives ; – Le contexte d'étude est souvent particulier ; – Les résultats ne sont pas généralisables ; – Le besoin d'une instrumentation assez lourde et parfois très longue.	– La recherche qualitative devrait : o être guidée par des considérations théoriques, plus que déterminée par des considérations techniques o se concentrer sur l'analyse de phénomènes contextualisés o se concentrer non sur les explications de faits, mais sur les explications de processus. – L'observateur est à la fois sujet et objet car il interfère avec les phénomènes observé. Il devrait en tenir compte dans la production d'informations et de connaissances.

Tableau 10 : Limites et particularités de la recherche qualitative

(Adapté de Haller 2014 p. 167)

4.2.2. Collecte et analyse des données

Nous présentons dans cette section le protocole de recueil et l'analyse du matériel empirique. L'objectif est notamment de répondre à la notion de fiabilité de la recherche qualitative conduite, qui repose principalement sur la « capacité et l'honnête du chercheur ». Cela nous conduit à décrire, pour une lecture critique, l'analyse de données brutes collectées puis transformées et simplifiées (Thiétart et al. 2003 p. 277 citant Miles et Huberman 2001). Il s'agit de détailler, d'une part, comment a été constitué notre échantillon de recherche et d'autre part, les stratégies d'accès au terrain, c'est-à-dire le dispositif de recueil de données primaires mis en place. Enfin, nous exposons la façon de coder et d'analyser nos verbatims.

Selon Miles et Huberman (2003 p. 58) les méthodes qualitatives reposent sur de « petits échantillons » qu'il convient d'étudier en profondeur en précisant leur contexte. Nous avons souscrit à leurs recommandations de choisir un échantillon « orienté » sans qu'ils soient pré-spécifiés. En effet nous nous intéressons à la décision d'adoption symbolique de la SSI par des acteurs disposant d'un niveau de **responsabilités au plus haut dans l'organisation**, tel que la littérature sur la SSI l'a explicité (cf. 2.4.1 « Gouvernance » p. 41). En revanche, nous n'avons pas pu constater l'effet que Miles et Huberman remarquent sur la chaine de recommandations des « informants ». Si nous avons systématiquement fait valoir l'intérêt que l'on portait à disposer de recommandations pour accéder à d'autres dirigeants, aucun des répondants n'a permis d'accéder à un autre. Nous avons pu activer une technique de « parrainage » par l'intervention de deux parrains qui ont permis la mise en relation avec des dirigeants qui pour certains ont accepté un entretien sur le sujet sensible de la SSI. Notons que selon Thiétart et al. (2003 p. 242) si « la confiance » des dirigeants à notre endroit e ne constitue pas une garantie quant à la qualité des données collectées, l'absence de confiance entraine un biais considérable ». Ainsi, le rôle du parrain est double pour nos travaux, d'une part un gain de temps considérable et une confiance favorisée puisque amenée par une personne « connue » du dirigeant. Malgré cette relation de parrainage et bien que plus d'une trentaine de dirigeants ont été contactés pour participer à nos travaux, seuls 17 ont finalement accepté, les autres ont décliné notre sollicitation ou n'ont pas

répondu à nos relances, peut-être à cause de la sensibilité du sujet, tel qu'évoqué par Kotulic et Clark (2004).

En outre, tel que le préconisent Guba et Lincoln (1989) nous avons pu constituer un échantillon à variation « maximale » (Miles et Huberman 2003 p. 61) en sélectionnant les répondants dans des secteurs d'activités différents. Cette variation ne porte que sur les secteurs d'activité car nous avons ciblé des décideurs de petite structure, dont un critère de choix est celui du dirigeant qui ne délègue pas ses problématiques de SI et de SSI.

Selon Miles et Huberman (2003 p. 59), la définition de l'échantillon en recherche qualitative implique trois points d'attentions particuliers. D'une part, il faut définir les caractéristiques des cas à étudier tout en s'assurant de disposer d'un échantillon qui puissent « porter » cette connaissance. D'autre part, « et dans le même temps », une structure doit se constituer pour « découvrir, qualifier ou confirmer » les construits sous-jacents à nos travaux. Enfin une pour chaque cas étudié il faut veiller à décrire chacun des processus observés afin de conserver la cohérence avec les théories mobilisées et ne pas introduire de biais dans l'interprétation.

Entretiens

Les premiers entretiens, comme évoqué dans l'introduction générale, ont été réalisés en amont de notre travail doctoral. Réalisés auprès de neuf responsables de la SSI, ils ont permis de faire émerger plusieurs conclusions qui ont alimenté notre réflexion pour la problématique. Notons que les résultats interprétés et discutés dans ce manuscrit ne reprennent pas les verbatims de ces neufs entretiens, même s'ils ont été établis sur les mêmes principes méthodologiques.

Les entretiens individuels ont été « semi-directifs », le principe adopté a été de laisser s'exprimer le répondant sans intervenir sur l'orientation du propos. Ce principe répond à la non-directivité nécessaire pour laisser s'exprimer l'interviewé car « chaque élément de son discours a une certaine valeur car il renvoie de façon directe ou indirecte à des éléments analytique de l'objet de recherche » (Thiétart et al. 2003 p. 235). Il permet aussi de ne pas écarter une possible **« heureuse trouvaille »** en dépassant les « a priori et les cadres théoriques initiaux » (Miles et Huberman 2003 p. 25). Ainsi nous avons souscrit aux recommandations de Thiétart et al. (2003) sur l'adoption d'une « attention positive inconditionnelle ».

Ainsi une fois les questions contextuelles posées au dirigeant sur l'activité et lui-même, la question majeure vise à le laisser s'exprimer sur son adoption symbolique de la SSI. Dans le détail, le guide d'entretien (en annexe) est basé sur les concepts d'AS déclinés à la SSI (cf. 3.4 « L'adoption symbolique adaptée à la gestion du risque » p. 193) en considérant l'adoption d'une bonne idée, la SSI sur les acceptions que nous rappelons : perception du besoin ; renseignement sur la solution ; évaluation de la solution. Les autres thèmes du guide sont corolaires à ces dernières acceptions et issus également des concepts d'AS déclinés à la SSI :

- SI et SSI
- Les risques pour le SI, le dirigeant et l'entreprise
- Influences isomorphiques pour la SSI
- Réponse au risque / mise en œuvre de la SSI

Précisément ces concepts ont été déclinés au travers de question sur les éléments suivants avec les objectifs associés :

Concepts déclinés en question	**Objectifs**
Éléments considérés lors de la décision	Identifier les éléments pris en compte et la connaissance par le dirigeant de ces éléments Identifier la prise en compte d'influences externes ?
Renseignements pris sur les risques et la SSI	Quelle connaissance a le dirigeant des **risques** SI qui peuvent l'impacter lui et son entreprise La connaissance mobilisée l'est-elle au profit de la SSI ? Quelle est l'origine de ces connaissances ?
Validation de la SSI	Quels éléments ont permis d'identifier la SSI comme « bonne idée »
Organisation de la sécurité	Quelle décision est prise pour ces risques ? Quelle déclinaison est établie sur les renseignements mobilisés La décision est-elle traduite ?

Tableau 11 : Objectif des thèmes en regard des questions

Ces entretiens ont eu une durée approximative d'une heure et demie, souvent, compte tenu des fonctions des interviewés, il a fallu réduire le temps prévu initialement. Comme le

recommandent Miles et Huberman (2003) nous avons pris soin, en début d'entretien, **de systématiquement définir la confidentialité des données recueillies**, assurer le gommage des mentions de marque ou d'entreprise dans les retranscriptions et le manuscrit, et la possibilité pour l'interviewé d'accéder à la retranscription, afin qu'il puisse apprécier lui-même le respect de ces règles. Également, nous avons été présentés majoritairement comme « praticien / chercheur » spécialiste en SSI et ainsi adossée aux règles de déontologie de la profession, dont la confidentialité est un des fondamentaux. Ces entretiens comprennent 28 heures de discours retranscrit et ont été reportés en environs 300 pages (cf. la retranscription d'un entretien en annexe).

La grille d'entretien a été élaborée selon une méthode visant la cohérence avec notre cadre théorique et notre design de recherche. Elle comprend ainsi, conformément au tableau 11, 4 catégories principales auxquelles s'ajoutent les questions de contexte (Éléments considérés lors de la décision ; Validation de la SSI ; Renseignements pris sur les risques et la SSI ; Organisation de la sécurité). Dans chacune des catégories sont positionnés les concepts théoriques. Les questions sont, dans le guide, précisées en regard des références académiques majeures de ces concepts. Enfin, certaines questions se recoupent pour assurer **l'exhaustivité et la cohérence des réponses données**.

Selon Glaser et Strauss, cités par Thiétart (2003 p. 216) la taille adéquate d'un échantillon est celle qui permet d'atteindre la saturation théorique… Cela signifie que dès lors que les informations, obtenues d'entretiens supplémentaires, capable d'enrichir la théorie la taille de l'échantillon est atteinte. Autrement dit, la collecte des données s'arrête lorsque les dernières unités d'observation analysée n'ont pas apporté d'éléments nouveaux.

Analyse et codage

Les données qualitatives sont souvent perçues, dans la littérature, comme plus difficile à traiter que les données quantitatives dans la mesure où elles sont soumises à l'interprétation du chercheur (Miles et Huberman 2003 ; Thiétart et al. 2003). Ainsi, dans un souci de traçabilité des résultats et de reproductibilité, notre objectif est d'expliciter les processus d'analyse que nous avons utilisés dans notre recherche.

Ainsi, la notion de catégorie dans le sens de la « valeur d'un thème » est soulignée Thiétart et al. (2003 p. 463). Il s'agit en effet de dessiner une structure d'un discours en formalisant les relations entre les différents thèmes qu'il contient dans une approche processuelle et interactionniste. Ainsi « l'analyse qualitative vise à interpréter la présence ou l'absence de

catégorie données, dans le contexte dressé lors du discours » afin « de comprendre comment elles sont utilisées » (Thiétart et al. 2003 p. 463) tel que sous-tendu par la définition de Yin (1989).

	Idées reçues…	**Implications directes et indirectes**	**Réponse du chercheur**
Quant à leur statut ontologique	Les données primaires ont un statut de vérité parce qu'elles proviennent directement du terrain	Excès de confiance dans les déclarations des acteurs Théories trop intuitives ou tautologiques	Les questions sont croisées et les données contextualisées Le cadre théorique est explicité et démontrer pour notre objet de recherche
Quant à leur impact sur la validité interne	Les données de première main ont une validité interne immédiate	L'excès de confiance dans la validité interne des données primaires pousse à éluder des explications rivales ou à ignorer des variables intermédiaires	La présentation de nos résultats et leur interprétation / discussion permettent d'apprécier les « explications rivales »
Quant à leur impact sur la validité externe	L'utilisation de données essentiellement primaires diminue la validité externe des résultats	On compense par des données secondaires qui n'ont pas de rapport avec la question onde recherche	Absence de données secondaires.
Quant à leur accessibilité	Les données primaires sont difficilement accessibles	On privilégie des données secondaires mais incomplètes alors que l'objet de la recherche mériterait le recueil de données primaires (heuristique du disponible)	Absence de données secondaires. L'accès au terrain pour un sujet aussi sensible a permis d'accéder à la saturation théorique
Quant à leur flexibilité	Les données primaires sont très flexibles	On s'embourbe dans le terrain par le manque de disponibilité des acteurs Travestissement des données primaires en les détournant de l'objet pour lequel elles ont été recueillies	La disponibilité des acteurs, dirigeant d'entreprise, a été un frein considérable qui n'a pas empêché à la saturation théorique. Une attention particulière a été portée au processus de codage

Tableau 12 : Idées reçues sur les données primaires

(Adapté de Thietart et al. 2003 p. 90)

Nous avons alors procédé selon deux étapes, un codage ouvert et un codage axial. Selon les recommandations de Gavard-Perret et al. (2008 p. 256) le codage a été réalisé par phrase entière ou morceaux de phrase et exploité ensuite par un « système organisé de rubriques et de catégories pour *in fine* affecter un code à chaque unité considérées. Nous avons observé avec attention les indications de (Thiétart et al. 2003 p. 90) sur les « idées reçues » sur les données primaires « afin d'éviter les biais ». Le codage ouvert (Thiétart et al. 2003 p. 177) consiste à « nommer et catégoriser les phénomènes grâce à un examen approfondi des données », pour les classer et les comparer pour ensuite donner un nom aux catégories constituée, désignées comme « in vivo ». À cette étape a succédé une phase de « codage axial » qui met l'accent sur les relations entre catégories et sous-catégories pour qui il s'agit de constituer des définitions de code avec les concepts de la littérature et ensuite de « spécifier chaque catégories en termes de causalité, contexte d'actions- interactions et de conséquences de ces dernières » (Thiétart et al. 2003 p. 177). Autrement dit, il s'agit de relier les codes obtenus avec les catégories issues de notre codage des thèmes de la littérature. Précisément, pour nos travaux, ce code revêt la forme directe de catégories et sous catégories issues de notre cadre théorique d'adoption symbolique adaptée à la SSI (cf. 3.4 « L'adoption symbolique adaptée à la gestion du risque » p. 193). Ainsi, en complément des catégories de notre grille de codage, par exemple, nous avons fait émerger une catégorie particulière, celles du rôle des prestataires informatiques des dirigeants dont il apparait que leur rôle d'influence soit associé positivement ou négativement sur les risques SI et la SSI.

Si Miles et Huberman (2003), préconisent plusieurs codages à différents intervalles de temps afin de limiter les biais inhérents au recours à un seul analyste, nous n'avons pas eu recours à un double codage et l'analyse des données repose uniquement sur notre propre interprétation. En accord avec le commentaire de Straub et Welke (1998), fort d'une expérience de plus de quinze ans en gestion du risque et en SSI, nous n'avons pas jugé pertinent d'effectuer un double codage, « au risque de mobiliser des ressources inutilement ». Enfin, nous avons entrepris une phase de « codage sélectif » au cours de laquelle nous avons analysés et interprétés les catégories majeures à l'aune des construits, concepts et théories identifiés.

Thèmes	Catégories	Sous-catégories
Contexte : SI et SSI	Importance du SI	Importance du SI pour le développement de l'activité, avantage concurrentiel… : – considéré comme stratégique – considéré comme support technique – en regard du secteur d'activité
	Importance de la SSI	Importance de la SSI pour l'entreprise Importance de la SSI dans le secteur d'activité Importance considérée du SI pour le développement de l'activité, avantage concurrentiel
Les risques pour le SI, le dirigeant et l'entreprise	Risque perçu	Risque : – imaginé – vécu personnellement – vécu par des proches – connu car « médiatisé »
	Menace	– exposition à la menace – menace endogène – menace exogène
	Conséquence	Nature des conséquences – sur l'entreprise – « Métier » – sur le dirigeant – technique sur le SI – directe sur le client
	Acceptation du risque	Sans ou avec contremesures de sécurité
Influences isomorphiques pour la SSI	Normative	Effet des réseaux professionnels et associatifs, de proches et de prestataires
	Coercitive	Effet de la loi ou de la réglementation
	Mimétique	Adoption des pratiques d'un concurrent

Thèmes	Catégories	Sous-catégories
Adoption symbolique	Perception du besoin	Le besoin de répondre à un risque
		D'autres besoins
	Renseignement sur la solution	Origine des renseignements
	Évaluation de la solution	Adaptions de la SSI au risque
	Raison de l'adoption symbolique	Représentation d'une « bonne idée »
Réponse au risque / mise en œuvre de la SSI	Absence de mise en œuvre	Contrainte matérielle
		Contrainte financière
		Absence de compétence
	Mise en œuvre	Mesure de sécurité technique
		Mesure de sécurité organisationnelle
		Compétences mobilisées
		Appui d'un prestataire informatique

Tableau 13 : Codage des thèmes

4.2.3. Rigueur du processus de recherche

Rappelons que les sciences de gestion se définissent par leur projet de « représenter de manière intelligible les interventions des acteurs au sein des organisations ou, plus précisément, ''d'identifier les processus cognitifs de conception par lesquels sont élaborées des stratégies d'actions organisationnelles possibles et par lesquels ces systèmes se finalisent, s'auto-représentent et mémorisent leurs actions et leurs projets dans des substrats qu'ils perçoivent complexes'' » (David 1999 p. 23 citant Le Moigne 1990). C'est justement ce que nous nous sommes attachés à développer dans l'ensemble de ce chapitre, afin de permettre la « critique réflexive » nécessaire à la démarche scientifique en gestion.

Selon Gavard-Perret et al. (2008), la légitimation des connaissances dans le paradigme épistémologique constructiviste pragmatique repose sur l'adéquation de la méthode mobilisée avec le projet de recherche poursuivi. Ainsi le travail épistémique ou « critique réflexive » est inhérent à la légitimation des connaissances. Pour plusieurs auteurs, il s'agit

de justifier l'enseignable et l'adéquation (Charreire et Huault 2001 ; Le Moigne 2012) que nous exposons avec la validité interne et externe.

Aussi, pour appréhender le critère **d'adéquation**, il convient de revenir au statut de la connaissance. Cette dernière n'est pas une représentation unique du monde réel. Elle doit être comprise comme une clé qui ouvre des voies possibles de compréhension. Autrement dit, une connaissance est « adéquate » si elle suffit, à un moment donné, à expliquer ou à maîtriser suffisamment finement une situation (Charreire et Huault 1999). Le degré d'adéquation reste à l'entière appréciation du chercheur, seul véritable expert sur le terrain (Von Glasersfeld 1988). Pour Avenier et Thomas (2015) la **justification de fiabilité**, aussi nommée « crédibilité » s'inscrit dans l'intelligibilité du cheminement cognitif à partir du matériau empirique (codages successifs, inférences…). Si le sujet connaissant exerce malgré lui et à son insu une influence dans le recueil d'information, alors la fiabilité consiste essentiellement à éclairer le lecteur sur les moyens suivis sur l'ensemble du cheminement cognitif conduisant du matériau empirique de la recherche (les données de la recherche jusqu'au résultat annoncés, Gavard-Perret 2012 p. 41). Rappelons ici que les expériences ne permettent pas de découvrir la « nature des choses en soi » mais sont seulement susceptibles d'évaluer l'adéquation des modèles du monde avec l'expérience empirique » (Von Glasersfeld 1988 p. 34).

Le critère d'enseignabilité est défendu par Le Moigne (2012) et se décline explicité en termes de reproductibilité et d'intelligibilité permettant alors la transmissibilité de la connaissance produite. En ce sens, pour notre projet dont l'objectif est à visée exploratoire, compréhensive et descriptive toute connaissance est construite de manière projective (Charreire et Huault 1999) et contextualisée, les rendant intelligibles dans un contexte spécifique. Ainsi nous nous sommes attachés à produire des connaissances qui favorisent l'émergence de représentations nouvelles pour la SSI en prenant soin de les contextualiser pour chaque cas étudier avant d'en produire une généralisation théorique et non pas statistique. La reproductibilité doit offrir la possibilité d'étendre les résultats obtenus sur l'échantillon à d'autres éléments, dans des conditions de lieu et de temps différents. Dans le cas d'une recherche qualitative, la généralisation statistique à un échantillon plus large n'est pas adaptée. Ainsi et conformément à notre posture constructiviste, le mode de généralisation des connaissances est celui de la généralisation conceptuelle qui amène à développer des connaissances dites « génériques » (Avenier et Gavard-Perret, 2012 p. 37). Ces auteures rappellent que l'élaboration de ces connaissances « repose sur un travail préliminaire de catégorisation par comparaison de diverses manifestations du phénomène étudié et

identification de leurs similarités et de leurs disparités (op. cit.). Il s'agit alors de mettre en action les connaissances élaborée dans une perspective d'action et non pas de mise à l'épreuve de leur validité. Ceci est établi, dans nos travaux, par une « une description épaisse susceptible de faciliter leur interprétation et leur adaptation a un autre contexte par l'acteur désireux de les mettre en action dans cet autre contexte (op. cit.).

Selon Thiétart et al. (2003 p. 277) la fiabilité de la recherche repose sur « la capacité et l'honnêteté du chercheur à décrie le processus de sa recherche », notamment sur le codage et l'analyse de données collectées. Ainsi, nous nous sommes efforcés, tout au long du projet, d'apporter une description large des techniques de collecte et d'analyse des données et par là de maintien de la chaine de preuves (Miles et Huberman 2003). Nous avons opéré une mise en résonnance de nos connaissances acquises par notre pratique professionnelle dans une attitude réflexive et des matériaux de données primaires issues des entretiens avec les décideurs. En ce sens, nous nous sommes continuellement interrogés sur le biais associé à un entretien sur la décision pour la SSI avec un « expert » de ce domaine. L'accès au terrain nécessite, pour les interviewés, de se remémorer les évènements et leur réflexion au début de la création de leur société ou le moment précis qu'ils indiquent comme étant « la décision pour la SSI ». Pour certains, cette réflexion a été conduite plus de dix ans en arrière, ce qui a nécessité de les interroger « en profondeur » sur ce « moment », sans toutefois avoir l'assurance de toujours disposer des informations recherchées.

Dans cette perspective, nous retenons que Miles et Huberman (2003 p. 78) indiquent qu'« en recherche qualitative, la validité et la fiabilité de l'instrument reposent largement sur les compétences du chercheur… c'est une personne -plus ou moins faillible- qui observe, interroge, et enregistre, tout en modifiant les outils d'observations, d'entretien et d'enregistrement d'une visite de terrain à une autre ». Par ailleurs, l'auteur ajoute qu'il s'agit pour le chercheur de décrire avec honnête et très concrètement le processus entier de sa recherche. Nous avons apporté une description complète de notre démarche tout au long du chapitre dédié aux choix épistémologiques et méthodologiques.

Chapitre 5. Résultats de la recherche

Ce chapitre est dédié à la présentation des résultats de notre recherche. Nous nous intéressons aux influences sur la décision d'adoption symbolique de la SSI par des dirigeants d'entreprise ou « top-managers ». Dans l'objectif de structurer ces résultats, nous les regroupons selon les catégories et sous-catégories développées dans notre plan de codage. À la fin de chaque catégorie, nous dressons une synthèse des verbatim les plus pertinents en regard de nos questions de recherche sous forme de tableau.

Les entretiens ont été conduits auprès de 17 dirigeants d'entreprise, dont les formes et les activités sont distinctes. Nous présentons à la suite de nos résultats un synoptique précisant l'AS de la SSI, contraintes à l'AS, connaissance et approche du risque et leur connaissance des solutions. En annexe une synthèse des caractéristiques de des entreprises de ces dirigeants sous forme de monographie

Nos résultats révèlent une perception des risques issus **prioritairement des risques vécus**, ensuite des risques partagés avec des proches ou des associations et enfin des risques imaginés. Notons en ce sens que presque tous ont vécu, soit en tant que dirigeant soit au titre d'une activité précédente, des situations à risque. En ce sens, les conséquences sont souvent évoquées lorsque les risques sont vécus, et moins développées lorsqu'il s'agit des autres risques. Notons également que l'exposition au risque, traitée dans la partie « menace » semble minorée en regard des commentaires des dirigeants.

L'acceptation du risque, quant à elle n'est évoquée qu'en regard des mesures de sécurité définies et mise en œuvre, ce qui la positionne théoriquement après l'adoption symbolique.

Les comportements isomorphiques sont mis en évidence sous l'angle coercitif, par les règlementations qui s'imposent au secteur d'activité ou au entreprise directement ; les effets de la concurrence et de la participation à des groupes semble peut émerger dans nos résultats.

Si les étapes de la décision d'adoption symbolique peuvent être conceptualisées dans nos résultats, ceux-ci font apparaitre que l'AS n'est pas un processus unique mais qu'il regroupe davantage une itération entre les phases.

Enfin, en complément de notre plan de codage, il nous a semblé pertinent de reporté les commentaires des dirigeants qui indique que nos échanges ont fait émerger, au moins, des questions sur leur sécurité des SI.

5.1. Contexte : SI et SSI

Avant d'aborder les risques pour le SI, l'entreprise et le dirigeant, nous exposons l'importance accordée par le dirigeant pour son SI pour l'activité de son entreprise et ensuite son regard sur la SSI pour son entreprise et plus globalement pour son secteur d'activité.

5.1.1. Importance du SI

Les verbatims indiquent que le système d'information **apparait comme important pour l'usage qui en est fai**t, en termes de finalité pour le dirigeant et dont il ne pourrait *« se passer »* :

- *D1 : « C'est un **élément indispensable car organisationnel** sinon on va très vite tomber dans un volume de candidats que la mémoire ne vas pas suffire à gérer »*
- *D2 : « …ce **sont des espaces partagés**, genre Dropbox, sûrement qui vont se mettre en place, pas quelque chose de très élaboré … il a **les fichiers clients avec la prod**, j'ai les **fichiers clients avec la partie administrative** ! […] c'est qu'on fait pas mal de **R&D ».***
- *D5 : **« …**un logiciel de gestion de cabinet d'assurance spécifique **qui me permet de gérer tout ça** … c'est un logiciel qui permet d'avoir des dossiers de **clients à jour tout le temps** donc à la fois une base clients et avec tous les courriers »*
- *D6 : « **Très importante** avec des bases de données de formulation de nos produits et les bases de données article, bases de données clients… la base de données de formulation c'est une base qui **comprend tout notre R&D** »*
- *D8 : « L'informatique a **pris un poids monstrueux dans les entreprises**, le mail a pris un poids monstrueux dans les entreprises. Je ne sais pas combien mais grosso modo moi, en traitement de mails par jour, en réception, je suis entre 60, 70 voire 80, sur lesquels il **faut apporter des réponses** ».*
- *D11 : « **Tout le développement de nos propres suites de notre écosystème**, logiciel au sens large et voix sur IP. »*
- *D16 : « Il a une **très grande importance** car c'est un outil qui nous permet de nous **coordonner à distance** car nous travaillons sur des lieux différents et à des moments différents. »*
- *D17 : « …comme on fait de l'événementiel, le SI, c'**est stratégique pour toutes nos activités** »*

Au-delà de l'importance soulignée pour le SI de cette entreprise, notons l'affect [65] énoncé par D8 : *« pour déterminer l'importance de mon SI, on peut quantifier le temps qu'on pourrait s'en passer : à mon avis, pas très longtemps ! Question d'heures à mon avis, peut-être de minutes… […] c'est* ***devenu évidemment très central*** *[…] j'ai un système et* ***j'y tiens comme à la prunelle de mes yeux ».***

Lorsque les réponses ne sont pas seulement orientées sur l'usage, le SI est aussi considéré comme un support à la conformité réglementaire et permettant d'apporter la preuve et la traçabilité des actions et décisions effectuées, par les dirigeants et par les clients :

- *D7 : «* ***déjà le SI, … c'est notre cœur de métier*** *en fait. Nous ne faisons que ça, traiter des données.* ***C'est au cœur de notre dispositif, un élément vital de la vie de mon entreprise » et «*** *le système d'information* ***me permet de prouver que j'ai bien rempli mon obligation de moyens****, accessoirement de résultat et que je fais juste » et « C'est très important parce que ça donne* ***le cadre à l'exercice professionnel*** *…, en respectant ce cadre qui est fait principalement de* ***déontologie et de règlementations****. »*
- *D9 : « …****si on ne conserve pas la justification*** *et qu'après on a une remise en cause par le client parce que ses intérêts ont changé, parce que ça l'arrange de dire l'inverse, ou je ne sais quoi d'autre, et bien il nous faudra faire la preuve que ce qu'on a fait, on l'a fait avec lui, par lui et par ses instructions »*

Dans le domaine de la santé, le SI a vu son rôle passer de « support informatique » à un moyen de réaliser les activités d'une part mais aussi surveillé par des autorités de régulations d'autre part, « *dont les données médicales et les patients sont au cœur* » :

> *D10 : « …l'informatique était une fonction support… aujourd'hui l'informatique devient un élément* ***central avec des experts visiteurs qui aujourd'hui regardent ça avec une très grande précision et ont des exigences beaucoup plus élevées*** *qu'il y a quelques années... »*

Un des interviewés, précise que son SI relève autant du traitement et stockage papier que numérique :

[65] Au sens de Finucane et al. 2000 et Slovic et Peters 2006

D14 : « Ce sont des registres à tenir comme dans toute entreprise : registre de sécurité, registre des produits phytosanitaires … On doit informatiser bien-sûr ! […] beaucoup de papier. Parce que le papier ça a des avantages aussi, ***beaucoup d'avantages****. […] C'est le suivi de l'activité. Comme dans toute entreprise,* ***c'est essentiel****. Le suivi des clients, le suivi de l'activité au jour le jour. »*

En ce sens, D15 évoque d'abord qu'il *« **ne stocke rien**, l'essentiel des informations est transmis verbalement […]. S'il le faut on note 2 ou 3 trucs sur un bout de papier mais c'est tout.* Il complète en indiquant que *« les seules informations dont on a la responsabilité c'est effectivement les cartes bancaires puisque sur chaque réservation aujourd'hui on a un numéro de carte bancaire »* puis de détailler l'origine de ses réservation *: « la réservation peut arriver par Booking, par Expédia, par mon site mail perso et par téléphone. Et par téléphone, je demande aussi les* ***coordonnées bancaires du client*** *qui me les donne sans problème 99% du temps. ».* La suite de l'entretien a permis d'identifier un classeur papier pour la gestion des réservations.

5.1.2. Importance de la SSI

Les verbatims indiquent principalement que la SSI est considérée comme importante, majoritairement par association avec l'activité même de l'entreprise :

- *D2 : « … on remet des rapports à nos clients, dans la partie amont « conseil » c'est souvent* ***confidentiel*** *[…] « par ex. l'année dernière, on nous a demandé et cela a même été imposé, de garder* ***le projet confidentiel*** *»*
- *D4 : « … différents côtés de sécurisation… Ensuite, il y a une sécurisation interne de l'entreprise, une sécurisation* ***que l'on doit à nos clients.*** *»*
- *D5 : « … pour moi c'est surtout la protection des données, la protection des données de mon propre cabinet en fait dans le sens où ce sont des milliers d'heures quand on les cumule pour le scan, la saisie d'information, de mises à jour, ça c'est une part* ***importante du fonds de commerce… si je perds ça demain c'est assez problématique !*** *»*
- *D7 : « … personnellement, j'agis par le management de la qualité donc j'ai normé ISO mon cabinet en 2004, … c'est-à-dire que normalement, je dis bien normalement, la manière dont on traite les données n'est pas faite au hasard » et « quand on entend la sécurité, pourquoi c'est* ***moi qui in fine la gère****, c'est parce que c'est une* ***question de***

responsabilité *! S'il y a une difficulté, une erreur, in fine,* ***c'est moi qui suis responsable****. »*

- *D8 : « 1 - Ne pas perdre d'informations donc principalement pour moi c'est* ***une remise en route de tous les systèmes en moins de 2 heures,***

  2 - ***Éviter la diffusion d'informations****, diffusion externe soit* ***sur la concurrence soit sur des clients en particuliers****. Je ne voudrais pas que des bases* ***clients puissent sortir de la structure ».***

- *D11 : « …la partie sécurité dans* ***ces systèmes est fondamentale****.. […] Elle était surtout centrée sur la sureté de fonctionnement, la disponibilité en fait* ***que le service soit toujours accessible*** *pour les centres d'appels »*
- *D9 : « Pour moi c'est la capacité de … se remettre au travail… si l'organisation a été* ***mise dans l'incapacité de travailler****. C'est-à-dire que* ***c'est le clash qui fait que tout s'arrête*** *: est-ce que je redémarre ou pas ? Dans quel état ? Sur combien de temps ? À quelle vitesse ? En mode dégradé ou pas ? »*
- *D16 : « Il s'agit de* ***protéger*** *nos informations des* ***virus, du vol, du détournement*** *et, tout simplement, des ennuis dus aux* ***pertes ;*** *si on perd ou on casse un ordi, un téléphone, moi, ma secrétaire, mes collaborateurs… »* et *« À mon sens, elle est* ***importante*** *sans être fondamentale »*

  D17 : « …c'est important de garder une trace de tous nos échanges parce qu'on peut oublier très vite et passer à côté de quelque chose sans même y faire attention » et *« …on met en place des événements pour nos clients, on leur fait du feed-back sur nos actions, donc nous devons faire très attention à la sécurité des données »*

D'autres commentaires suggèrent que la SSI est considérée comme importante car elle permet de se différencier des concurrents et peut être mise en avant comme argument de vente :

- *D2 : « Nous on se servirait volontiers de* ***l'argument de vente*** *auprès de nos clients… contrairement à 99% de nos concurrents qui, quand ils ont un QR Code sur les photos, cela renvoie à* ***toutes les photos de l'événement****, nous, dès le départ on a dit ce n'est pas possible et on en a fait un argument de vente »*
- *D4 : « :.. ensuite, il y a une sécurisation interne de l'entreprise, une sécurisation* ***que l'on doit à nos clients. »***

On note qu'un des interviewés (D3) évoque l'absence de paranoïa lorsqu'il s'agit de la SSI et le système « *informatique* ». L'importance de la SSI lui est clairement apparue après un incident qui l'a conduit à prendre LA décision de protéger son système « informatique », qui a été « impacté » malgré des mesures techniques mises en œuvre par son prestataire. *« Je ne suis pas* ***quelqu'un de parano****, absolument pas et donc j'ai envie de dire pour moi ça n'avait que très peu d'importance,* ***que très très peu d'importance*** *… » et après « Ça a pris de l'importance quand il* ***y a un an on a pris un virus ransomware et là on s'est dit ''oh, alors là c'est la m…, vraiment !''*** *À partir de là j'ai* ***pris des décisions pour sécuriser notre système informatique*** *mais pas tant en termes de mots de passe et de choses comme ça parce que la société informatique que j'emploie nous avait dit qu'on a un Cisco et que c'est vachement bien... bon on a quand* ***même pris un ransomware*** *».* D16 fait un lien directe entre décision et prise de conscience des risques *« Et donc quand j'ai pris conscience de ça, je me suis dit qu'il fallait* ***protéger nos informations des risques*** *qui pouvaient nous tomber dessus.* ***J'ai pris plusieurs décisions sur le matériel, la protection des données, la mémorisation et les sauvegardes aussi. J'ai pensé aussi à informer et un peu à former mes salariés…)***

Certains des réponses sur l'importance de la SSI considérée se distinguent de celles autres interviewés, D6 répond ainsi à ces deux questions :

- Qu'est-ce que la sécurité des systèmes d'information pour vous :

  « Rien du tout,… voilà c'est clair, j'ai un antivirus… »

- Quelles dispositions avez-vous prise au moment de cette attaque ?

  « Je sais pas j'ai pas le temps de m'occuper de ça je joue avec le feu mais je n'ai pas le temps… »

Pour compléter ultérieurement par…

> *D6 : « … oui je* ***faisais de la sauvegarde*** *des fichiers stratégiques sur Hubic ou des sauvegardes sur disques externes. » et « … sans rentrer dans les détails* ***j'ai rentré les droits d'accès*** *parce que j'ai vu une deuxième personne qui avait accès à ces dossiers et c'est pas normal que je le fasse aujourd'hui… »*

Pour un interviewé, dont le cœur de métier ne repose que sur le stockage, le traitement et la diffusion d'information délivrée et dont la pertinence est évaluée par le seul client, la SSI n'est pas importante parce que déléguée.

> *D12 : « On va dire que je suis plus intéressé* ***par les pratiques de sécurité de ma voiture*** *que de ma boîte, c'est con hein… ? »*
>
> *D12 : « je* ***lui ai fait une totale confiance*** *sur le sujet donc je* ***ne m'y suis pas plus intéressé*** *que ça… »*

À la fin de l'entretien, il souligne l'importance d'un « pack de sensibilisation » à la SSI à destination des nouveaux « start-upper » :

– Le start upper validerait un pack sensibilisation comme celui que vous décrivez, comment le feriez-vous passer ?

> *D12 :* ***: «*** *Oui, en le* ***sensibilisant au risque****, tel que le pompage, la disponibilité du site Web, …, mais dire que ce sont des choses qui se pensent rapidement, que les collaborateurs peuvent changer, que changer les mots de passe ça va vite etc etc,* ***je pense que ce serait très intéressant****… »*

En complément, l'importance de la SSI est évoquée pour le secteur d'activité les réponses sont centrée sur la réponse aux exigences réglementaires imposée par les autorités de régulations de l'activité concernée :

> *D1 : « C'est un sujet très peu abordé, sur lequel il y a peu… de toute façon il y a une transgression par rapport à la loi même telle qu'elle a été faite 10 ans en arrière … » et « mais globalement je pense que la* ***profession est très mauvaise parce qu'il n'y a pas d'obligation****, il y en a une qui arrive avec GDPR mais* ***il y a peu de problématique*** *autour de ça et à mon sens,* ***peu de scandale médiatisé historique*** *propre au recrutement lui-même… » et « j'ai eu un numéro d'agrément (de la CNIL) sachant que cette base de données depuis 2009* ***a beaucoup évolué*** *depuis on ne m'a jamais rien redemander et j'ai toujours* ***mon agrément ad vitam aeternam*** *(rire) »*
>
> *D9 :« …c'est le* ***secret professionnel*** *qui fait qu'effectivement on doit avoir une notion de l'information qu'on protège, qu'on sécurise, qu'on ne divulgue pas, etc... et la protection face* ***à une mise en responsabilité****, c'est-à-dire de conserver des données*

qui ont permis de mettre en place des situations, mise en place que ***l'on pourrait nous reprocher ensuite*** *si on n'arrivait pas à justifier des données correspondantes. »*

D15 : « Après les seules informations dont on a la responsabilité c'est effectivement les ***cartes bancaires*** *puisque sur chaque réservation aujourd'hui on a un numéro de carte bancaire… sur certaines réservations où on a toutes les informations y compris le* ***cryptogramme*** *»… « donc la seule information* ***vraiment importante concerne*** *effectivement les* ***coordonnées des clients avec l'adresse, l'adresse mail et le numéro de carte bancaire. »***

5.1.3. Synthèse de l'importance des SI et de la SSI

Les SI apparaissent comme étant au cœur des activités des organisations dont nous avons interviewé les dirigeants, que ce soit pour une activité dont le SI est un support technique ou qu'il ait un rôle « stratégique » pour le développement de l'activité. Ainsi l'usage de ce SI est souligné par plusieurs dirigeants, notamment par le fait qu'ils ne pourraient pas *« s'en passer »*. En complément l'apport des SI apparait comme central dans les organisations soumises à des réglementations sur des données spécifiques telles que les données de santé, mais aussi plus largement pour les organisations qui doivent assurer leur fonctionnement dans un cadre « *qui est fait principalement de déontologie et de règlementations* ». Notons que l'importance des SI qui ressort des entretiens est en ligne avec le choix de notre terrain, visant à ne pas considérer les organisations dont l'intérêt pour son SI n'est pas majeur, autrement dit à ne pas interviewer de dirigeant dont l'activité ne repose pas sur le SI.

La SSI, quant à elle, est considérée comme importante voire très importante, ou encore « *fondamentale »* en regard de l'activité de l'organisation et dans le prolongement des commentaires sur l'importance du SI. Soulignons les verbatims qui montrent que la SSI, pour un des dirigeants, jusqu'alors tenue comme ayant « *que très très peu d'importance »* prend une importance différente dès lors que l'entreprise est impactée par un cryptolocker qui a provoqué la perte de *« 40 ans de données parce qu'on a un serveur qui a été crypté complètement et qu'on ne récupèrera jamais* », appelant le commentaire *« du coup on a redonné un peu plus d'attention » (à la SSI).* L'importance de la SSI se révèle aussi par la description de la sécurité du service ou des données livrés ou utilisés par les clients de ces organisations. Seuls deux interviewés (D6 et D12) n'indiquent pas directement l'importance qu'ils accordent à la SSI, bien qu'une lecture approfondie des entretiens fasse émerger soit

des pratiques, soit des recommandations, très centrées sur la protection des SI. Enfin, l'importance de la SSI est évoquée par nécessité, pour le dirigeant, de se conformer aux exigences réglementaires qui lui sont imposées tout en notant que les interviewés souscrivent à ces principes de protection. Par exemple D10 indique qu'en « *cas de non-respect de la règle c'est énorme très clairement et aussi un risque pénal car nos patients peuvent nous attaquer si on n'a pas fait en sorte d'assurer la confidentialité de leurs données* ».

Contexte SI et SSI	
Importance du SI	*« C'est un élément indispensable car organisationnel… »* *« Très importante avec des bases de données de formulation de nos produits et les bases de données article, bases de données clients… »* *« …j'y tiens comme à la prunelle de mes yeux ».* *« C'est au cœur de notre dispositif, un élément vital de la vie de mon entreprise »*
Importance de la SSI	*« ..cela a même été imposé, de garder le projet confidentiel »* *« ..c'est une part importante du fonds de commerce… si je perds ça demain c'est assez problématique ! »* *« la partie sécurité dans ces systèmes est fondamentale »* *« si l'organisation a été mise dans l'incapacité de travailler, c'est une remise en route de tous les systèmes en moins de 2 heures »* *« la partie sécurité dans ces systèmes est fondamentale »* *« elle était surtout centrée sur la sureté de fonctionnement, la disponibilité en fait que le service soit toujours accessible pour les centres d'appels »*

Tableau 14 : Synthèse des verbatims sur l'importance des SI et de la SSI

5.2. Les risques pour le SI, le dirigeant et l'entreprise

En accord avec la littérature et la grille de codage que nous avons élaborée, nous présentons les risques en 4 parties définies selon les déterminants, soit les risques perçus, les menaces considérées, les conséquences et, enfin, les risques acceptés.

5.2.1. Les risques perçus

Dans cette **première** partie des résultats, nous présentons les risques perçus, qu'ils soient imaginés, vécus personnellement ou par des proches. Nous présentons d'abords les **risques imaginés** en termes de **risque** « brut », de **perte de donnée ou de service**, de **piratage**, ou encore, pour une minorité, par **l'absence de sauvegarde**.

Les risques perçus imaginés

Les risques perçus imaginés et évoqués par les dirigeants dans cette première sous-partie ne sont pas « qualifiés », c'est-à-dire, qu'il s'agit de risques pour lesquels la menace, l'exposition et les conséquences ne sont pas formelles (risque « brut ») :

> *D3 : « Oui, peut-être que je devrais couvrir le risque de foudre mais alors il faudrait que je couvre aussi le risque d'inondation, d'incendie, de…* ***on ne peut pas parer à tout ça quoi*** *! Moi* ***je me dis que j'ai autre chose à faire que de m'inquiéter et ça ne m'inquiète pas****. … en 40 ans ce n'est pas arrivé et je ne vois pas pourquoi ça arriverait maintenant. Oui c'est* ***un risque hypothétique****. »*
>
> *D4 : « C'est assez étrange d'ailleurs ces problèmes de sécurité parce qu'en fait on est sensibilisé au niveau personnel, et* ***on s'aperçoit finalement que dans toutes les entreprises que j'ai pu voir, en fait, elles sont moins bien sécurisées*** *que nos propres données personnelles. […] C'est-à-dire que finalement tout le monde apporte des clés USB, transmet des mails, les postes ne sont pas forcément avec des anti-virus, etc… Mais ça* ***c'est global à toutes les entreprises c'est malheureux****. »*
>
> *D4 : « …une* ***philosophie sécuritaire*** *pérennité de notre société, c'est-à-dire que si on ne sécurise pas certaines données, comme le paiement, comme la gestion avec la Douane, etc… on met en péril l'activité. Donc il faut* ***absolument sécuriser cela****. »*

*D7 : « J'ai depuis longtemps mené des réflexions. Déjà, j'ai **essayé de segmenter les risques** c'est-à-dire que je ne me suis pas mise comme chez beaucoup de confrères, dans une seule tour pour réunir tout le monde pour faire des économies. »*

*D9 : « Pour moi un SI qui fonctionne supporte les deux métiers : je pense qu'on ne peut justifier qu'il fonctionne que par la présence … **d'un schéma où il faut de temps en temps se mettre en faux péril,** … comme quand on fait des exercices d'alerte nucléaire ou d'incendie c'est bien pour tester ce qui fonctionne et ce qui ne fonctionne pas… **Sinon c'est compliqué de se dire on va attendre l'accident** pour voir si on est capable de déclencher un plan blanc. »*

*D13 : « C'est comme ça que je fonctionne en général quand je vois **qu'il y a un petit truc qui est arrivé** parce que tant qu'on ne sait pas, on fait rien ! »*

*D14 : « C'est un poste ''**fermé'' : il n'y a ni internet, ni rien,** par sécurité…. C'est le cœur de mon métier, j'y ai tous mes clients, mes contacts. J'ai voulu que ce soit à part, qu'il n'y ait que moi qui ai accès… […] Et j'ai **ressenti** le besoin de vraiment séparer les activités. »*

*D14 : « Et puis ce n'est que **du bon sens, rien d'autre**. Il faut bien **se protéger, si le système est fermé il sera plus sécurisé que s'il est ouvert**. »*

*D16 : « … on peut **perdre** des données, diffuser des données qui ne devaient pas l'être, se **faire piller par la concurrence**, se faire mal voir des auditeurs ou des organismes avec qui on travaille. »*

D17 : « ...il y a toujours quelqu'un pour mettre une clé, donner des infos au tél, envoyer un rapport par mail. Moi-même je ne suis pas toujours attentif et des fois je veux faire vite... »

Le risque SI imaginé est évoqué, par les dirigeants, dans la perspective d'une **perte de données ou de la nécessité d'assurer le fonctionnement d'un service adossé au SI**, voire la perte physique des données et du matériel informatique. Les causes de ces pertes relèvent, dans cette partie, principalement de menaces externes environnementales ou externes malveillantes telles un virus :

*D1 : « En me disant c'est une **sorte de revenu** en me disant il ne faut pas que ça ''crame'' et j'aurais tendance à dire que ces craintes proviennent plus de l'idée que la*

maison prenne feu ou qu'elle soit cambriolée et qui provoquerait ***la perte de tout ce qui a de la valeur*** *»*

D1 : « … c'est assez marrant, je vous avoue que je viens de réaliser un truc que je n'avais jamais conceptualiser avant mais c'est vrai qu'en ***parlant piratage industriel*** *… je suis presque plus* ***inquiet*** *par quelqu'un qui fouillerait mes poubelles que par quelqu'un qui rentre sur mon cloud et* ***d'ailleurs j'ai une déchiqueteuse****, qui vaut ce que ça vaut, parce que c'est toujours pareil ça devient compliqué et chiant, mais ça m'est déjà arrivé comme je pense dans n'importe quelle société de jeter un bon de commande que j'ai en doublon, une facture client qui est renvoyée, que normalement je déchire en deux et que je mets dans la poubelle potentiellement là-dessus vous savez avec qui je travaille il y a dessus de l'info, beaucoup d'infos, et finalement ça on n'en parle plus.. »*

D2 : « Quand on parle de l'ordinateur, ***c'est arrivé à un copain*** *qui est allé déjeuner, il a laissé son ordinateur dans la voiture, il s'est fait ouvrir la voiture et piquer l'ordinateur. Il s'est posé la question : est-ce qu'on m'a suivi ? Est-ce que c'est mon ordinateur, l'ordinateur de moi, l'entrepreneur de la boîte, qui a été visé ? Il faut le faire quoi, sur une zone commerciale, se faire ouvrir la voiture pour piquer un PC. Ça arrive vite, tu te fais piquer un vélo comme ça quand j'étais gamin… Voilà. Il y a* ***ce qu'on entend et ce qu'on a vécu****. … Donc* ***je suis assez sensible à ça,*** *au fait que* ***ça arrive très très vite et qu'on ne peut pas le voir venir****. »*

D3 : « … il y a ***un an on a pris un virus ransomware*** *et là on s'est dit ''oh, alors là c'est la m…, vraiment !'' À partir de là j'ai pris des décisions pour sécuriser notre système informatique ».*

D5 : « On ***risquait de tout perdre en fait, s'il y a un vol tout le matériel pourrait disparaitre,*** *comme pour un incendie, mais cela peut-être un dégât des eaux ce peut être tout, des aléas qu'on ne maîtrise pas… »*

D5 : « Au fil des discussions avec mon prestataire et mon cabinet comptable, … on a les mêmes problématiques en fait et je crois qu'il y a ***une transmission d'angoisse****… aussi on s'aperçoit que* ***quelle que soit la profession, en tout cas dans ces professions là, ce serait vraiment dramatique*** *effectivement* ***de perdre des données*** *»*

D6 : « … pas grand-chose à part que mes sites Internet seraient bloqués ou sursaturés ce qui est plus classique et puis sinon le système bloqué avec une demande de rançon ce doit être tout ce ***que j'imagine comme risque****… »*

*D7 : « Moi ce serait principalement la **fiabilité** du système informatique. Pas l'information, l'informatique. **L'intrusion d'un virus qui me foutrait en l'air mon truc**. »*

*D7 : « … je suis sûre qu'aujourd'hui, je me mets sur mon réseau, j'appuie sur les boutons **pour scratcher les données j'y arrive** ! J'ai des sauvegardes mais je voudrais éviter qu'on puisse faire ça. »*

D11 : (concernant le service délivré au client par les ressources SI et télécom) *: « …des thématiques où la **disponibilité du service est essentielle**, donc dès le départ il fallait trouver une solution qui nous permette de rendre le plus sécurisé possible l'accès à la ressource. »*

*D12 : « Après je touche du bois on a jamais **eu de gros problèmes en huit ans** d'existence. »*

*D13 : « … après on peut nous **mettre un virus** dedans pour que toutes nos données soit bousillées si quelqu'un nous en voudrait il nous **enverrait un truc et on bousille** votre système, après je n'ai pas de recul la dessus mais **j'imagine que ça peut se faire**… »*

D14 : (à propos des documents papier) *« Déjà au niveau sécurité, à moins que ça brûle mais voyez j'ai une armoire ignifugée ».*

*D16 : « Le gros problème, c'est **les virus** ou la **perte** involontaire d'informations de quelqu'un de chez nous… Perdre, ça peut nous mettre dans **une très mauvaise position, outre la perte de temps.** »*

Le risque SI est ici évoqué par les dirigeants en termes de **menaces externes malveillantes**, soit **une volonté d'atteindre le fonctionnement de leur SI** ou la disponibilité de leurs données et services, soit par exemple un piratage :

*D1 : « **Le pire des risques** ce serait le piratage des données qui sont censées être confidentielles et internes se **retrouvent plus ou moins publiques** cela va être le pire des scénarios … »*

*D1 : « La dernière préoccupation c'est **que cette base de données** est quelque chose qui est un petit peu embêtant parce que c'est une porte ouverte, tu peux être victime d'un piratage ou autre chose … (hésitation) mais plus inquiet **d'un risque de piratage** et que ces données se retrouvent dans la nature avec potentiellement à terme un usage*

malveillant c'est vrai que ma préoccupation c'est plus côté sauvegarde sécurité que je la fasse où je veux quand je veux… »

D2 : « Il n'y a pas d'atteinte à l'intégrité de la personne sur ces photos-là, … car c'est l'image du client qui est engagée !... Ce qu'il pourrait y avoir, en termes de fuites si on venait à capter notre base de photos c'est des photos compromettantes et qu'elles soient utilisées de manière malveillante. Cela fait beaucoup de si. Globalement on ***n'est pas vraiment inquiétés*** *».*

D2 : « Aujourd'hui et cela fait 8 ans qu'on existe, ***on n'a pas eu ce type de problème-là****… : de fuites, de se faire pirater notre banque de données. Je ne sais pas, c'est purement de* ***l'imagination****. Je* ***ne sais pas quel problème on pourrait avoir****… »*

D4 : « Au niveau de la sécurité je pense que ça se fait au fur et à mesure. Moi je suis très ''web'', très achats web et du coup je ***suis très sensible sur la sécurisation 3D****, l'aval de ma banque lorsque je donne, c'est surtout au* ***niveau des paiements****. C'est vrai que j'ai un regard sur ma situation personnelle en tant que sécurité mais c'est un avis de ma part. »*

D4 : « C'est ce qui me vient de suite à l'esprit, c'est une info générale j'ai envie de dire : ***tout le monde dit qu'il faut changer fréquemment****. Après le problème est aussi que sur tous les sites j'ai* ***le même mot de passe avec le même e-mail et je me dis que si une fois une base de données a une brèche****, la personne elle peut aller sur tous mes comptes et ce sera la même chose. »*

D9 : « ***C'est ça le risque****. La violation du secret professionnel c'est ça, c'est la* ***diffusion d'informations sensées être secrètes****. »*

D10 : « …depuis un véhicule des gars avaient ***piraté le wi-fi*** *et étaient rentrés dans notre SI administratif … et en fait, avaient* ***récupéré des données qui était dans ce SI*** *»*

D13 : (évoquant la récupération de ses données par un concurrent) ***« le fichier propriétaire*** *où il y a toutes leurs adresses et les coordonnées dont on peut* ***nous piquer*** *toute la gestion donc là il faut se protéger par rapport au piratage ! »*

D14 : « Je ***connais les risques de base*** *:* ***piratage****, virus, destruction. Voilà. Après il y en a certainement qu'on ne connait pas, qu'on a* ***du mal à appréhender. On ne connaît pas tous les risques*** *en fait. »*

Certains risques sont traduits non pas par la perte de donnée directe mais la perte des sauvegardes :

> *D1 : « … je suis photographe amateur je pense que **c'est arrivé à beaucoup de gens** de perdre une carte ou qu'une carte s'efface ou alors le CD qui ne se lit plus et qui conduit à multiplier les supports **pour ne pas avoir qu'une seule sauvegarde** du fichier **auquel je suis sensible**. »*
>
> *D8 : « D'abord la perte de données pure et dure qui m'inquiète parce que **si on n'a pas assez de back-up** […], tu as beau avoir 4 sauvegardes si tu n'en as pas une sur un site distant, ça ne sert à rien. »*
>
> *D6 : « **La perte de données déjà ne serait-ce que le backup** … »*
>
> *D9 : « … c'est les données. Si on a un vrai clash, les bureaux brûlent, tout brûle… le seul problème c'est que les **sauvegardes qui sont sur place auraient par définition** disparu mais elles sont **sauvegardées aussi à l'extérieur**. »*

Les risques perçus vécus personnellement

Dans cette seconde sous-partie, nous retranscrivons les risques que les dirigeants ont vécus personnellement. Ils sont majoritairement exprimés par la conséquence de perte de données ou de service et de piratage.

Les risques perçus vécus et évoqués par les dirigeants relèvent de la perte de données vécue ou évitée « de justesse » :

> *D1 : « Par **rapport à mon expérience**, non je n'ai jamais été victime de cambriolage ou d'une maison qui brûle ni de disque dur qui pète **mais oui victime à l'époque des CD beaucoup** ; si j'essaye de faire une prospective c'est vrai que les CDs étaient quand même un support assez fragile finalement peut-être plus que les disquettes même si j'ai moins bien connu cette période où **j'ai perdu des photos qui étaient sur le CD** ou un film téléchargé des choses comme ça ou même un logiciel dont le point exe est sur CD et ce **CD devient illisible alors qu'on pensait qu'il était bien sauvegardé** et puis voilà ».*

D2 : (suite à une question sur les raisons de réaliser une sauvegarde) *« **Suite au crash quand j'étais étudiant :** … je me remets à bosser et là j'appuie sur la barre d'espace pour remettre l'ordinateur en route, l'écran se lance noir puis d'un coup bleu puis plus rien. **Et là c'est le vide absolu**. …. J'ai **perdu 3 ans de photos, de cours, travaux. Je n'avais aucune sauvegarde, rien du tout. »***

*D3 : « Je ne **suis peut-être pas sensible à ce discours**-là. …quand j'ai pris la décision de faire ça, c'est que j'avais **été confronté au problème »***

*D3 : (le prestataire conseillant sur la sauvegarde externe) « …m'a dit tu fais comme tu veux, moi je t'ai prévenu ! […] Et là **c'est ma faute parce que le prestataire informatique m'avait dit quand même il faudrait que tu déportes ta sauvegarde, c'est important**. »*

D3 : « …2 fois on a eu le truc (le virus cryptolocker)*. La première fois en même temps que tout le monde et puis une deuxième fois l'année dernière, je ne sais plus exactement… […] par contre là comme on avait mis la sauvegarde en place, on n'a pas été trop embêtés. Mais la première fois on a bien été embêtés… Là je me suis rendu compte **qu'effectivement sauvegarder ses données c'était quelque chose de très important, très très important**. […] « La première fois on a perdu 40 ans de données parce qu'on a un serveur qui a été crypté complètement et qu'on ne récupèrera jamais. »*

*D3 : « Oui. Je **pense que je n'avais pas du tout conscience de ce que cela pouvait impliquer**. Quand **on a été touchés par le ransomware, ça nous a bloqué tout le serveur**. Par chance, … il y avait une sauvegarde qui se faisait dans le menu racine et le ransomware n'a pas pu aller là-dedans. … on a **perdu tous les fichiers qui étaient sur le serveur**. »*

*D4 : « …je parlais des sauvegardes que l'on fait sur du disque dur et où on essaie d'être assez fréquents. Mais dans une de mes expériences professionnelles précédentes, j'ai **déjà planté 1 mois et demi de travail comme ça** ! Alors là j'essaie de ne pas le faire tous les mois et demi mais on n'est jamais à l'abri de cramer son disque dur et que finalement c'est terminé et là ce **serait assez dramatique quoi**. »… « … **j'ai pleuré**. C'est certainement un virus, l'ordinateur n'a pas pu démarrer. »*

*D5 : « Ce dont on **a pris conscience** à ce moment-là c'est l'importance de ces données, quand on s'est rendu compte … on a scanné pendant trois jours quelque chose qui ne*

s'est jamais sauvegardé …mais ça nous a fait ***prendre conscience*** *qu'il fallait* ***peut-être sauvegarder les données*** *parce qu'on s'est dit que si on venait à perdre des jours des jours des jours comme ça … ce* ***serait des milliers d'heures de perdues »***

D7 : « Après oui, il pourrait y avoir d'autres risques : ***que mon cabinet brûle !*** *Je fais normalement* ***des sauvegardes à l'extérieur*** *»*

D7 : « Parce que je me dis qu'à un moment ou à un autre si… ***ça m'est déjà arrivé ici que mon serveur plante.*** *Et bien mes filles en social elles ne sont pas bloquées, elles se connectent à Ollioules et ça marche. »*

D9 : « un jour, on a eu un incident, ***le prestataire s'est aperçu par hasard*** *-et heureusement pas sous un mode de crise mais simplement en allant voir un truc- que les mails n'étaient plus sauvegardés depuis 6 mois avant.*

D16 : « On ***parle trop et les idées que l'on a se diffusent et partent à la concurrence****. J'ai eu, il y a quelques années, l'idée d'une nouvelle formation particulière sur un nouveau secteur très très prometteur : on n'a pas eu le temps de la mettre en place mais nos concurrents, avec qui ont eu des échanges, n'ont pas hésité eux. Ils nous ont bien* ***grillés sur ce coup****. »*

D16 : « On ***a diffusé des trucs qui ne fallait*** *pas mais on a toujours rattrapé le coup auprès des personnes concernées. Enfin, jusqu'à présent ! »*

D17 : « Chez moi, j'ai pris la foudre et j'ai ma box TV qui a pété. ***Donc, ça peut arriver****. »*

Les risques perçus vécus par les dirigeants relèvent de l'action malveillante volontaire, soit le « **piratage** » :

D6 : « On a eu 2 ou 3 fois des ***attaques*** *sur notre site Internet, jusqu'à maintenant j'ai eu* ***beaucoup de chance j'ai jamais eu de problème****… »*

D8 : « il y a 3-4 ans, on s'est ***retrouvés avec l'intégralité du tableau de commande produits d'un de nos concurrents*** *pour ses magasins… toutes les références, toutes les désignations, tous les modes de packaging et tous les coûts de produits » (à cause d'un stagiaire qui a publié ce tableau)*

*D11 : « on s'est rendu compte que ce **commercial travaillait dans notre dos** et pouvait même reprendre des propositions à son compte […] avec **récupération de clients** après donc ça c'est un premier cas.*

*D11 : « il n'avait aucune notion de la sécurité donc il utilisait des VPN privés depuis son poste pour pouvoir contourner notre fire-wall interne etc… […] et du jour au lendemain c'est devenu une catastrophe ! Bon on s'en est séparé **mais n'empêche que là j'ai vu tout le risque** et là on a vraiment perdu du temps pour tout remettre d'équerre et **donc là ça a été vraiment pour moi une prise de conscience** on m'ne avait déjà parlé que le risque finalement est beaucoup plus important en interne qu'en externe »*

*D12 : (sur l'utilisation frauduleuse des ressources de l'organisation) « on **ne comprenait pas** parce qu'un jour on a reçu un message d'alerte de cet hébergeur qui nous a dit ''**votre serveur a servi à attaquer le serveur de Sony** et donc on a dû vous suspendre l'utilisation de votre système''**.** L'administrateur système qu'on avait à l'époque a cherché et dans ce module en natif il y avait une porte dérobée qui permettait à des gens de passer par le serveur donc bien sûr on l'a fermée, entre-temps on utilise plus ce système **donc voilà, on avance comme ça…** »*

*D16 : « Des formateurs avec qui nous travaillons **nous en ont beaucoup parlé.** C'est vrai qu'ils sont un peu paranos parfois ! Enfin, il me semble. Peut-être qu'ils ont raison. »*

Notons dans les risques vécus, que D15 a été victime d'un vol : *« je me suis fait, il y a très longtemps d'ailleurs, presque 20 ans, piquer mes papiers, ma carte bancaire, débiter de plusieurs milliers d'euros, remboursés intégralement par la banque mais pendant 8-15 jours **on transpire un peu quoi…** »*

Les risques vécus par des proches

Dans cette troisième sous-partie, les dirigeants ont indiqué les échanges d'informations sur les risques qu'ils pouvaient avoir, certains ont directement évoqué les risques que les membres de leurs cercles « proches » ont rencontrés ou sur lesquels des prestataires ont attiré leur attention :

*D1 : « …on a tous quelqu'un qui râle parce qu'il a **perdu les données pas forcément pro** et je pense que ça fait partie de cette ambiance collective, une prise de conscience pour certains, … »*

D1 : « Il y a forcément des ***échanges avec des gens de cercle proche ou moins proche d'ailleurs qui vont vous raconter une expérience malencontreuse*** *et où on se dit il aurait pu m'arriver la même chose, je n'aurais pas été mieux loti et donc on peut essayer de s'en préoccuper, après les choses se font je pense de manière un peu empirique »*

D2 : « … c'est l'actualité : un cambriolage, mes voisins derrière chez moi volés 2 fois en 6 mois. C'est ça ce qu'on entend : on ne l'a pas vécu mais on l'a entendu, ***ça s'est passé à proximité****. »*

D3 : « On me citait des exemples : des bâtiments qui avaient brûlé, des vols, des choses comme ça des bâtiments… »

D5 : « Il s'est passé ***qu'on s'est intéressés au rachat d'un cabinet*** *pour opérer une croissance externe […]* ***ils ont connu un problème de perte de données*** *et donc cela* ***m'a fait prendre conscience que*** *cela a complètement désorganisé le cabinet »… « je me suis dit que s'il nous arrivait la même chose* ***ce serait assez catastrophique*** *donc aujourd'hui pour moi c'est une priorité que de sauvegarder ces fameuses données. »*

D6 : « un ordinateur qui tombe en panne ***ça arrive à tout le monde****… j'ai* ***plusieurs personnes qui ont eu un ordinateur qui tombe en panne*** *même si dedans il y avait pas de données stratégiques »*

D8 : (sur les informations transmises par un ami « spécialiste ») *« le deuxième truc sur lequel* ***il m'a alerté****, … c'est le nombre de* ***sauvegardes et la réitération des sauvegardes*** *avec différents types de sauvegardes et surtout de ne jamais avoir confiance dans les sauvegardes de back-up classiques qui te font des ISO et le jour où tu ouvres ton iso tu te rends compte qu'ils sont complètement en vrac parce que le serveur ''est pourri'' ».*

D8 : (sur l'éclairage sur les risque de la part des prestataires) *«* ***Je pense que oui****. Suffisamment, je ne sais pas mais je pense que oui.* ***Peut-être pas suffisamment, peut-être pas de manière trop négative mais oui****, encore une fois, que ce soit sur la partie antivirus avant, sécurisation, sur la partie craquage d'un Wifi, craquage des données, les ransomware…)*

D9 : « Il y a nos amis avocats, en dessous, qui se sont ***fait pirater parce que l'une de leurs assistantes a téléchargé une recette*** *de cuisine à sur un site ''cuisinons.com'' ».*

D9 : « ***Les expériences des voisins****,* ***partenaires, amis qui*** *se font piquer leurs données, qui perdent leur informatique, qui se font pirater leur système et qui se font*

*demander une rançon, etc., etc… tout ça fait que l'on se dit ''**et moi, si ça m'arrivait demain, comment je gère** ?'' »*

*D13 : « Quand on est jeune on fait des choses et on pense que rien va nous arriver, **après on voit qui a des choses qui arrivent à des copains qui perdent un disque dur qui a cramé ne serait-ce que des amis qui perdent le contenu de leur téléphone parce que ce n'est pas enregistré** et donc on se dit on va mettre des choses de sécurité pour pouvoir pallier à cette perte de données… »*

*D13 : « … j'ai des **particuliers et des professionnels** dans mon entourage donc **je suis assez à l'écoute de ce qui se passe et des expériences** et moi je me dis que l'expérience de quelqu'un va me servir à moi c'est pour ça que c'est fait je pense… et du coup lui il a eu ça moi je vais vérifier ce que j'ai et je regarde si c'est bon ou si ça peut m'arriver aussi donc à ce moment-là je me renseigne et là on me dit effectivement ça arrive donc on peut voir ce qu'on peut faire pour toi… et on peut voir si on peut mettre ça ou ça en place. »*

*D13 : « C'est comme ça que je fonctionne en général quand je vois qu'il y a un petit truc qui est arrivé parce **que tant qu'on sait pas, on fait rien**. Tant qu'il ne nous est pas arrivé ou **qu'il n'est pas arrivé à quelqu'un d'autre on ne l'imagine pas…** »*

*D16 : « Comme je n'ai pas trop de temps et de ressources, j'essaie surtout **d'écouter les mauvaises histoires des autres et de m'y' adapter** en interne pour éviter les même problèmes et les mêmes conséquences ! »* (par exemple *: « Il y a plusieurs des écoles avec qui nous travaillons qui se sont fait **détourner des informations sur leurs étudiants** ! Ça, ça craint. Je veux éviter cela à tout prix. »)*

Les risques connus car « médiatisés »

Cette quatrième sous-partie présente l'origine de la connaissance de certains risques sur lesquels des associations ou des clubs ont réalisé des communications :

*D2 : « Je pense que cela te maintient un peu en veille **d'entendre des choses**. Il y aussi le **journal télévisé où tu entends ces histoires de piratage et de demande de rançons**. Je me dis que nous on ne pourrait pas payer. Mais si on venait à grossir, il faut peut-être se poser la question. Donc ça fait réfléchir, ça maintient un climat et c'est vraiment le même sentiment que par rapport au cambriolage : on n'y pense pas, puis on*

entend un voisin, on a un cousin qui habite en Bretagne à qui s'est arrivé qui en parle. ***Ça maintient en veille*** *»*

D6 : « … il y a ***toujours des réunions d'information sur la vigilance sécurité*** *informatique par les associations des chefs d'entreprise auquel je suis adhérent bien souvent ce genre de choses » et « je fais* ***partie d'un club où il y a régulièrement*** *des* ***gens qui informent*** *les autres sur* ***les risques*** *et voilà … »*

D8 : (à propos des informations sur la sécurité transmise par son prestataire) : « …il ***y a des choses dont j'ai entendu parler et qui ont l'avantage de me mettre la conscience dessus****. »*

D8 : « Je m'en soucie un ***peu plus depuis quelques temps*** *parce qu'on* ***entend parler de plus en plus de ransomware*** *et surtout sur des petites structures ce qui m'inquiète un peu. »*

D9 : « Après, il y a une expérience malheureuse du cabinet d'avocats qui a été pris en ***otage par son propre prestataire informatique*** *sur la région*[66] *»*

D11 : « … sur la partie télécom pour le risque qui est colossale parce que beaucoup ***de boîtes ont coulé à cause de ça…*** *»*

D11 : (évoquant les problématiques que les principaux fournisseurs en France assurent couvrir) *« c'est déjà très largement tout ce qui est* ***risque machine****,* ***risque dans les DC****, les accès électriques, des accès Web »*

D16 : « J'ai entendu pas ***mal d'histoires*** *d'entreprise qui avaient eu de gros problèmes de sécurité de l'information ... »*

D17 : « …il y a ***tellement d'histoires*** *que l'on entend autour de nous, de clients, de fournisseurs, de concurrents aussi.* ***Dans les médias aussi****. À la fin, on peut avoir l'impression de devenir* ***parano****. »*

[66] « Comment ce cabinet d'avocats a été victime d'une cyberattaque » : il s'agit de trois membres d'une société de prestations informatiques remerciée qui ont porté atteinte au système d'information de son ancien client pour « montrer à leur ancien client que leur nouveau prestataire n'était pas à la hauteur. » (cf. http://www.varmatin.com/justice/comment-ce-cabinet-davocats-a-ete-victime-dune-cyberattaque-16304 consulté le 18 juillet 2018)

5.2.2. Les menaces

Dans cette seconde partie il s'agit d'aborder les menaces et l'exposition à ces menaces perçues des dirigeants, ainsi que leur nature « endogène » ou « exogène ».

Menaces et exposition

Cette première sous-partie présente à la fois le type de menaces considérées par les dirigeants et également leur regard sur l'exposition à ces menaces :

> *D1 : « **Alors de piratage pas vraiment** parce que **d'abord je ne suis pas une multinationale** et je **ne pense pas être la cible numéro 1** … je ne suis pas à l'abri d'un point de vue de sécurité des locaux, je ne suis pas à l'abri d'un cambriolage alors ce n'est pas particulièrement peu sécurisé mais ce **n'est pas une banque**… »*
>
> *D1 : « Si je pars en vacances, je vais avoir l'idée de prendre une sauvegarde avec moi et d'en laisser une autre à mes parents et mon ordinateur à la maison, mais là demain je vais acheter une baguette de pain et ma maison brule entre temps, je ne **m'amuse pas tous les jours à mener** la dernière sauvegarde à mes parents, à me trimbaler un disque dur dans mon sac à dos, alors il y a **toujours un petit risque** ».*
>
> *D1 : « Alors peut-être qu'effectivement l'audit qui est prévu d'être réalisé par cet ami va révéler que **je me berce d'illusions** sur la sécurité des données c'est même très vraisemblable mais en tout cas, je n'ai pas eu de consultation de quiconque sur la manière dont je protège mes données. »*
>
> *D2 : « Mais je ne sais pas si c'est bien de tout avoir au même endroit ! **J'ai l'impression** qu'on est **un peu dans le minimalisme**, dans l'amateurisme dans ce qu'on fait. On fait le minimum mais j'ai l'impression qu'en **fait on couvre assez bien notre sujet, notre sauvegarde**. »*
>
> *D3 : « ….je n'ai plus les exemples précis en tête mais je sais **qu'on n'arrivait pas à entrer sur le serveur …** On n'était pas capables de dire en interne que si eux ne nous répondent pas qu'est-ce qu'on fait ? Vous ne rentrez pas **sur votre serveur, enfin ça ce n'est plus possible** »*
>
> *D3 : « Pour moi, **je ne voyais pas qui pourrait nous hacker** : notre société fait 1 million de CA max, on ne pèse rien. Sauf que **je n'avais pas pensé** au ransomware. »*

D7 : (au sujet de l'impossibilité de disposer de son SI pour assurer la conformité) *« **Pourquoi une aversion au risque** ? Parce que, en permanence, aujourd'hui, parce qu'on est dans une **société totalement déresponsabilisée**, déraisonnable. Quand un petit s'est fait mal à la tête parce qu'il a pris le poteau, ce n'est pas le petit qui n'avait pas de casque ou qui était au mauvais endroit, c'est le poteau qui est au mauvais endroit »*

*D7 : « Alors si tout brûle, il **faudrait que j'aie un ennemi**.. ».*

D7 : (au sujet des raisons de la vérification des méthodes et procédures de son prestataire) *: « Parce qu'à un moment il **peut y avoir une panne sèche**. Ce qu'on v**eut éviter c'est que quand l'avion est en l'air, il se scratche même si c'est une chance sur un million**. Voilà ! »*

*D9 : « Après je suis conscient **qu'on n'est pas à l'abri d'un problème**…. Et que si ça doit péter un jour, la théorie de l'emmerdement maximum étant ce qu'elle est, il est probable que ça pète [...] C'est comme la ceinture de sécurité : on ne la met pas parce qu'il y a la police, on la met parce **que si un jour il y a un carton**, il sera forcément à 130 à l'heure, de face et que ce jour-là il vaudra mieux avoir la ceinture que pas l'avoir, ne serait-ce que parce que les dégâts seront moins lourds que ce qu'ils pourraient être si la ceinture n'est pas mise. »*

D12 : (en parlant de l'exposition aux menaces) *« Après je **touche du bois** on a jamais eu de gros problèmes en huit ans d'existence […] et « on fait de l'espionnage donc par définition y'a que James Bond qui est un espion qui se fait voir, nous **on est plutôt en mode discret donc je pense que ça joue**… »*

Les menaces exogènes

Cette seconde sous-partie permet de distinguer les menaces retenues par les dirigeants et provenant de l'extérieur de leur organisation :

*D3 : « …des bâtiments qui avaient brûlé, des vols, des choses comme ça. Mais nous ça fait 40 ans… **je touche du bois** … on n'a pas eu de problème majeur là-dessus, **donc pourquoi ça arriverait ?***

*D3 : (sur la menace environnementale) « Parce que je n'y **pense pas, mais pas du tout !** Effectivement, **si la foudre tombe là**, **on est pratiquement sûrs et certains que le serveur qui est juste là il charge**. C'est clair, c'est sûr. Mais non, mais… »*

D4 : « Donc très clairement, c'est le ***cœur de notre business*** *(le Web)* ***et qu'on soit dépendants que d'une entrée, ça paraît complètement fou****. Donc vraiment je crois que la première action elle serait là-dessus.* ***C'est vraiment là-dessus où on n'est pas bons !*** *»*

D5 : « Mais il suffirait qu'il y ait ***un individu malintentionné*** *qui vienne juste pour prendre le matériel ce n'est pas le matériel en soi qui me pose problème c'est ce qu'il y a dedans donc le* ***risque absolu est là, c'est le vol, l'incendie****… »*

D6 : (sur les raison qui le poussent à sauvegarder) *« Par peur de casser mon ordi ou de le* ***perdre*** *ou qu'on me le* ***vole*** *».*

D6 : « …mais ce ne serait pas la fin du monde car toutes les sauvegardes sont sur disque dur… ce serait quand même ***la faute à pas de chance*** *que le même jour et je* ***me plante et la maison brûle*** *et celle de mon comptable qui a* ***disque dur brûle aussi*** *».*

D6 : « …je pense que quelqu'un qui veut attaquer la sauvegarde physique de mon disque dur que j'ai faite et qui est planquée chez moi ou chez mon comptable, ***elle est un peu plus dur*** *à faire* ***que celle d'un truc qui passe par le réseau****, quel que soit le VPN le mot de passe etc… »*

D7 : « C'est comme une maison, vous avez beau mettre un portail, toutes les protections, et bien le ***pépin*** *il va* ***venir dans la faille que vous n'avait pas vue****. Je suis convaincue que vous ne pouvez voir la faille que si régulièrement* ***vous avez des gens de l'extérieur qui viennent regarder le truc.*** *»*

D8 : « D'abord la perte de données pure et dure qui m'inquiète parce que si on n'a pas assez de back-up et que ***tout brûle au même endroit****, tu as beau avoir 4 sauvegardes si tu n'en as pas une sur un site distant, tu ''pisses dans un violon'', ça ne sert à rien. »*

D8 : « Moi ça (le ransomware) *m'inquiète, alors peut-être* ***un peu trop mais oui ça m'inquiète parce que ce n'est pas trop*** *l'argent, parce qu'en général les mecs ne réclament pas des grosses sommes. On leur file 3.000 € et on* ***n'est quand même jamais sûr de les récupérer*** *nos données ! Et si on les récupère, est-ce qu'on les récupère en bon état ? Là est toute la question et je ne sais pas bien… »*

D12 : « …et pour le moment je ***retouche du bois*** *parce qu'il n'y a pas de problème »*

D13 : « …ça reste toujours cette petite peur de la concurrence qui viendrait me faire un piratage de mes données … […] Quelqu'un pourrait essayer de travailler avec le propriétaire, essayer de le contacter, essayer ***de le prendre en gestion*** *voilà… »*

D13 : (au sujet des données sauvegarde sur une clé et stockée dans une agence immobilière) *« Oui mais uniquement si on a le logiciel pour* ***les exploiter*** *sinon il y a rien qui sera exploitable et sur un autre ordinateur il n'y a rien qui se sera accessible… »*

D16 : « *Je ne* ***pense pas que l'on soit espionnés*** *par d'autres personnes ou des organisations ou des concurrents… »* mais *« On parle trop et les idées que l'on a se diffusent et partent à la concurrence […] on n'a pas eu le temps de la mettre en place mais nos* ***concurrents****, avec qui ont eu des échanges, n'ont pas hésité eux »*

D17 : « Alors on fait des sauvegardes des données mais on n'est quand ***même pas une entreprise secret-défense****. On se protège à peu près même si on reste un peu artisanal en ce qui concerne la sécurité »*

Les menaces endogènes

Cette troisième sous-partie permet de distinguer les menaces retenues par les dirigeants et provenant de l'intérieur de leur organisation, mettant en lumière le rôle des prestataires informatique :

D6 : « … parce que je ne suis pas très ***content de mon prestataire*** *de service qui manage tout ça, j'en suis même plutôt mécontent, et* ***j'ai découvert moi par hasard****, parce que je me suis posé la question, que* ***les sauvegardes ne se faisaient plus*** *donc* ***j'étais en roue libre, au total sans savoir depuis combien de temps ça a duré****… »*

D8 : (le stagiaire informaticien) *« C'est* ***toujours ma crainte aussi****, notamment quand j'ai des stagiaires comme ça […] je suis obligé de lui donner les mots de passe serveur, etc… parce qu'il a besoin d'accès [...]. donc à partir du moment où il s'en va, qu'est-ce que je mets en place pour éviter que le garçon puisse devenir* ***potentiellement un problème demain matin*** *?* ***Qu'est-ce qu'il a pu faire*** *que je ne* ***maîtrise pas du tout*** *sur nos installations informatiques ? ».*

D8 : « Je ne suis pas à l'abri que ***mon gentil prestataire****, que je connais depuis un* ***an, joue au casino demain et soit pris à la gorge financièrement****, qu'il ait besoin de pognon et qu'il monte tout un système pour hacker tous ses clients.* ***On n'est jamais à l'abri de cela*** *! »*

D10 : « …on s'est aperçu qu'il avait encore accès à des informations extrêmement sensibles et que clairement il pouvait ***nous planter du jour au lendemain*** *»*

D11 : « …un de mes ingénieur qui a un moment a commencé ***à faire vraiment des grosses grosses conneries, à saccager une partie de nos codes*** *sur le SVM, à saccager des éléments importants de notre informatique à vouloir même ouvrir des VPN, parce qu'il n'avait aucune notion de la sécurité, donc il utilisait des VPN privés depuis son poste pour pouvoir contourner notre fire-wall interne etc…* ***donc quelqu'un d'assez folklorique et malheureusement j'ai eu tort de reconduire sa période d'essai*** *et du jour au lendemain* ***c'est devenu une catastrophe*** *! Bon on s'en est séparé mais n'empêche que* ***là j'ai vu tout le risque*** *»*

D12 : « …la personne qui est parti, ***on avait une totale confiance en elle*** *et* ***elle a pas été très clean*** *parce qu'elle est partie en mode ''j'ai envie de voir autre chose'' et en fait elle m'a écrit un mail un mois après en disant* ***'je t'aimais pas je te supporte plus*** *et ça fait un mois que je suis parti et j'ai encore mes accès'', on avait pas vraiment modifié ses accès parce qu'on se disait ''on va les lui laisser,* ***il est sympa, peut-être que demain il peut nous donner un coup de main sur la résolution d'un problème…''*** *»*

D12 : (évoquant la gestion des mots de passe des collaborateurs et de l'important turn-over de personnel*) « **On est jamais parfait** il faudrait **qu'on s'améliore**, qu'on soit plus **proactifs** sur certains points, on pourrait avoir des choses un petit peu centralisées »*

D16 : « …la perte involontaire d'informations de quelqu'un de chez nous… Perdre, ça peut nous mettre dans une très ***mauvaise position, outre la perte de temps****. »*

D17 : « Faut faire encore plus attention en interne qu'en externe [...] …un problème compliqué, c'est le salarié qui transmet une info sans faire exprès ou qui quitte l'entreprise avec des fichiers… Ça, c'est possible mais c'est compliqué de le stopper «

5.2.3. Les conséquences des risques

Comme nous l'avons plusieurs fois pointé dans la littérature, il serait incomplet de présenter des risques sans évoquer les conséquences. Celles-ci peuvent concerner directement la viabilité de l'entreprise et / ou, les fonctions métier, et / ou le dirigeant.

Les conséquences directes sur l'entreprise

La majorité des conséquences des risques abordées lors des entretiens relèvent d'un impact sur l'entreprise elle-même :

> *D1 :* (conséquence de la perte irréversible des données) *« Si je reste sur quelque chose de chiffrée, je ne sais pas mais une perte de CA qui est assez difficilement quantifiable, il faut le reconnaitre, je* ***sais pas mais 20 %, ce qui reste une estimation approximative*** *mais parce que force est de constaté qu'il y d'autres cabinets de recrutement qui s'installent et qui n'ont pas non plus une inertie de 10 ans avant d'arriver au niveau du CA que je peux générer »*
>
> *D1 : « Cela serait* ***l'anéantissement de l'ancienneté*** *et de tout ce que ça peut apporter dans mon activité, cela veut dire reparti à zéro… Alors certes sur les process déjà pensés et établis pourraient se remettre en place très vite mais le contenu, les CV, le contenu de cette base de données seraient perdu et d'une importance… »*
>
> *D2 : «* ***je dirais 30%*** *parce que c'est ce qui doit correspondre à peu près au taux de clients qui ne sont pas fidélisés, ceux qui ne vont pas te laisser une deuxième chance, qui ne vont pas comprendre, ceux qui n'ayant pas la réponse dans les 48h* ***vont fermer la porte et aller voir ailleurs*** *»*
>
> *D2 : «* ***je ne vais pas dire ''on ferme la boutique''.*** *Non.* ***Ça pourrait aller jusque-là*** *mais non parce que j'aurais une sauvegarde. Mais si je perdais l'ordi et la sauvegarde et le téléphone, donc tout,* ***je ne sais pas ce qu'il pourrait se passer****. Il y aurait beaucoup d'efforts à faire, ce serait une reconsidération complète, un nouveau plan d'actions, tu refais une nouvelle feuille de match. Tu refais tout quoi. Tu as une équipe, tu as 10 blessés sur 15, il faut tout refaire.* ***C'est ce sentiment****. […] Si on perdait tout,* ***j'aurais tendance à croire qu'on ne fermerait pas la boîte*** *c'est sûr, parce que quand même les données principales restent stockées dans des mails. »*
>
> *D3 : « Et le disque dur externe de sauvegarde une chose que je ne savais pas. […]* ***Et les clients aussi parce qu'on a perdu aussi une semaine de travail*** *sur tout ce qui était devis et facturation. »*
>
> *D3 : « En fait, les* ***conséquences j'ai envie de dire qu'on les a découvertes au fur et à mesure****, c'est-à-dire au départ on n'a pas pensé à tout, on ne s'est pas dit « tiens il y a ça, il y a ça et ça ». On a vu certainement le principal et après, de temps en temps, en se disant ''on aurait besoin de ça, on ne le trouve pas...'' **Ah ! D'accord, ça remonte à ça** !*

Mais sur le moment, non, ***on n'a pas forcément imaginé tout ce que ça pouvait impliquer. »***

D4 : « … le ***risque de perte d'exploitation et ensuite le risque de l'accès du client*** *au site de vente et le risque de dépréciation du service (c'est concernant le mail et concernant aussi l'accès):* ***quand un site est ralenti c'est pénible et donne une mauvaise image****, quand le* ***service client ne répond pas, on a une mauvaise image****, etc, etc… »*

D5 : « ***Je crois qu'ils ont perdu trois ou quatre mois de CA****, ils ont consacré trois à quatre mois de l'année à ne faire plus que ça c'est-à-dire que récupérer les données, ils n'ont plus travaillé » il n'y a pas eu d'extension et pas de croissance sur le plan financier* ***ça peut coûter très cher… »***

D6 : « … je ne sais pas. J'appellerais mon prestataire en lui demandant comment cela est possible sachant tout ce qui me coûte, je lui paye un antivirus, un machin et ***voilà j'attends ça de mon prestataire et sinon je restaurerais les informations de la veille*** *et au moins je* ***n'aurais perdu que le delta*** *»*

D7 : « Alors si tout brûle, il faudrait que j'aie un ennemi. Donc j'ai quelqu'un qui me brûle tous mes cabinets. ***Normalement, avec un ordinateur, je suis censée pouvoir récupérer toutes mes données****. »*

D8 : « ***Donc la perte d'informations qui peut mettre tout le monde au chômage****, ça ça* ***m'a toujours inquiété*** *et le temps passé à remettre un système. Là je ne parle pas d'un bâtiment brûlé mais d'un serveur qui se fout en vrac. »*

D8 : (sur le cout d'un incident) *« … on va retomber sur nos pattes, on va en sortir mais ça peut être un coût de 30, 40 ou 50 K€ d'opérations en temps passé, en temps perdu à reconstituer. J'ai des données là-dedans qui sont tellement vieilles… aujourd'hui on fait 2 M€ de CA, donc 2,5% à 3% du CA… » et « parce qu'on est* ***super tendus depuis*** *des années et que c'est* ***le genre de choses qui nous coûterait trop cher****. »*

D9 : « Je ne vis pas dans l'inquiétude car je me dis qu'au pire on perdrait, parce qu'on perdrait forcément, j'ai du mal à croire qu'on restaurerait tout immédiatement, 1 semaine, 2 semaines, 3 semaines de boulot, ***je ne nous vois pas couler****. »*

D11 : « Si jamais on coupe le téléphone vient à rencontrer un ***dysfonctionnement*** *les personnes* ***sont immédiatement au chômage technique*** *! »*

D11 : « …et là vous vous retrouvez avec une note que vous allez devoir régler et qui peut être ***de 200 ou 300 000 € en une nuit****, c'est énorme ! […] le risque qui est colossale parce que* ***beaucoup de boîte ont coulé à cause de ça*** *»*

D13 : « quelqu'un pourrait ***essayer de travailler avec le propriétaire, essayer de le contacter, essayer de le prendre en gestion voilà****… parce qu'un bien qui est en location là, le propriétaire habite pas là, donc c'est très compliqué d'avoir les coordonnées d'un propriétaire… donc si vous* ***avez facilement accès à cette base*** *vous pouvez les contacter vous savez les gens qui démarrent peuvent proposer un tarif plus bas que le mien en faisant valoir l'intérêt pour le client donc "****venez chez moi****" »*

D16 : « En y réfléchissant, il peut y avoir aussi l'envoi d'informations à des personnes qui n'auraient pas dû les recevoir. Ça peut arriver aussi. On brasse tellement d'informations avec les mails, les fichiers, etc. que ***le risque est d'envoyer des choses plus ou moins confidentielles à des personnes qui peuvent ensuite continuer à les diffuser****. »*

D17 : « …c'est peut-être pas fatal mais ça peut faire très très mal à l'entreprise, sur le chiffre d'affaires, etc. […] sans parler des problèmes où on perd des données et doit s'arrêter de travailler pendant une heure ou un jour complet »

Les conséquences « métier »

Moins engageantes et plus ciblées que les conséquences pour l'entreprise, les conséquences métier mettent en perspective les impacts sur certaines fonctions de l'entreprise :

D3 : « Ça nous est arrivé d'être dans l'incapacité ***de travailler sur une demi-journée par exemple et de voir que ce n'était pas gérable*** *quoi, c'était* ***très très compliqué*** *parce qu'on perd du temps. »*

D5 : « Quand on perd la connexion un matin, mis à part les dossiers papiers des urgences que je peux avoir sur mon bureau, ***je ne peux plus travailler*** *»*

D6 : « j'aurais ***perdu une semaine de boulot****… c'est surtout* ***des heures de perdues*** *et un risque d'oublier ce qu'on a fait quand on fait les choses c'est écrit il faut qu'on les fasse et on les oublie si on perd l'ordi* ***on sait plus ce qu'on a fait****… » … « Donc si ça m'arrivait ce serait une perte de temps et la perte du travail, la* ***perte totale de ce qui a pu être fait entre la dernière sauvegarde et le moment de l'accident*** *»*

D8 : « Ce n'est pas arrivé souvent mais il y a 3 ans, ***on plante un PC à Sanary****. Ce que je fais, vu que c'est des fichiers donc normalement les fichiers ne sont pas ré-importables facilement, donc on réinstalle le logiciel mais on ne pouvait pas reprendre les bases de données telles quelles pour les remettre. […] Donc là-dessus, on réinstalle et je dis au prestataire : ''vous me refaites la redescente !''». La dernière sauvegarde elle avait 3 mois chez eux et quand je vois ça, je leur dis ''mais où sont toutes mes données depuis 3 mois-là ?'' Réponse : '' ah oui oui, mais en fait il n'y a pas de sauvegarde '*

D9 : « … et donc depuis 6 mois, les mails n'étaient pas sauvegardés. Et donc, si on avait eu un clash à ce moment-là et que ***mes mails disparaissaient****, on n'était pas capables de ressortir les mails. Ça pose le problème de faire et de vérifier ce qu'on a fait. »*

D10 : (les pirates) « avaient récupéré ***des données qui était dans ce SI*** *parce qu'à l'époque le dossier patient n'était pas informatisé …* ***dans le dossier administratif, il y a des données nominatives de patien****t.. »*

D17 : « Ça craint par ce que sur un mauvais coup on peut ***perdre un bon client*** *[…] … une fois, on a eu un problème de machines et on a perdu des heures et des heures alors que l'on était à la bourre. [...] une autre fois on a perdu des données, c'est rageant, il a fallu tout refaire la travail »*

Les conséquences directes sur le dirigeant

Certaines conséquences, au-delà de la nuisance provoquée à l'entreprise ou aux fonctions métier, touchent directement le dirigeant :

D3 : « on a perdu tous nos fichiers d'information, nos fichiers fournisseurs, sur les produits, etc…. tout a été perdu. Et là par contre je me suis dit ah, ça pose problème. ***Et puis, même si les fournisseurs sont assez compréhensifs, c'était assez gênant pour moi de devoir les contacter pour leur dire de me renvoyer une base de prix*** *parce qu'on ne l'a plus. Avec tout ce que cela implique pour certains fournisseurs parce que la base de prix ne va pas forcément être la même.* ***Donc ça c'était assez gênant. »***

D3 : « Quand vous devez appeler un client pour lui dire pouvez-vous me renvoyer votre bon de commande parce qu'on ne sait pas où il est passé, même si vous dites on a eu un problème informatique, ***c'est une position embêtante****. Le client peut comprendre mais il peut aussi se dire tiens, ils ne sont pas* ***en capacité de recouvrer ces informations et ça ne fait pas vraiment très professionnel.*** *À l'époque c'est ce que j'ai pensé. Pour*

moi, commercialement, cela devient une position de faiblesse en fait. ***Ce n'est pas une situation avec laquelle j'étais à l'aise.***

D6 : « mais moi ***c'est mon entreprise donc je suis plus sensible à l'impact du chiffre d'affaires*** *ou* ***de l'activité perdue si*** *ça m'arrive… »*

Les conséquences techniques sur le SI

Les conséquences techniques sont peu représentées dans les verbatims :

D3 : « Parce qu'on en parle oui. Après au quotidien je n'ai pas le temps. J'ai plus pris le temps de sécuriser en fait nos données, la redondance de nos sauvegardes que de dire en amont je mets ça en place. Moi ***je croyais qu'avec CISCO c'était bon, mais en fait on m'a expliqué que non.*** *»*

Les conséquences directes sur le client

Aucun des verbatims ne traitent de conséquences potentielles directes pour le client.

5.2.4. Acceptation du risque

Les verbatims qui relèvent de l'acceptation du risque montrent la volonté d'accepter la situation risquée, soit sans prendre de mesures de protection, soit avec des mesures existantes et qui apparaissent suffisantes pour le dirigeant :

D4 : « …j'avoue qu'on est moins sécurisé là-dessus…. ***puisqu'en fait la base c'est du papier, des dessins****. C'est stocké ici et si demain on ouvre nos locaux,* ***c'est accessible facilement****… on est sur un secteur qui en fait est très mode et du coup très saisonnier et on* ***change tellement souvent que finalement, oui copiez nous mais dans 5 mois ça ne sera déjà plus ça*** *! […]* ***c'est presque volontaire****, ce n'est pas quelque chose sur lequel on met l'accent parce que finalement si on a accès à ces données-là,* ***ce n'est pas très très grave !*** *[…] je pense au côté virus sur ordinateur, le côté disque dur planté … tout le monde en fait se dit que ça peut arriver et finalement on en accepte le risque. On l'accepte puisqu'on ne fait rien pour le contrer. »*

D5 : « …après les données sont protégées aussi parce qu'il y a un serveur qui vient piquer des données de chaque poste en ***permanence une sauvegarde en fait***

automatique, *il m'est déjà arrivé de perdre des données mais on les a récupérées facilement puisqu'on est allés puiser dans les sauvegardes… »*

D7 : « Mais ce sur quoi je ne suis pas rassurée, ***c'est que j'aurais aimé faire un audit****, pas de mes procédures (elles sont déjà auditées) mais de la sécurité* ***informatique du dispositif****. … Parce que je pense que mon interlocuteur raconte des c… »*

D14 : « tout brûle, tout explose… j'ai un deuxième bureau en fait, ça c'est mon bureau disons commercial et j'ai un bureau de travail… ça permet d'avoir ses papiers avec soi, de traiter ses papiers, de les copier si on a besoin, d'archiver. ***Avec l'informatique, on peut être soumis à des virus, des attaques, des pannes****.* ***Nous on n'est pas experts. Le papier on arrive à le gérer !*** *».*

D14 : « on a des contraintes climatiques, on travaille à l'extérieur, il y a des pannes, etc… Tout ça fait qu'au final les crises font partie de notre métier et on apprend à les gérer avec le temps. ***Des fois ça se passe bien, des fois il y a des problèmes*** *»*

D15 : « …le seul système de sécurité que j'ai mis en place à un moment, vraiment c'était basique, c'était le broyeur parce qu'effectivement ces ***numéros de CB qui se baladent c'est ''moyen''*** *».*

D17 : « … comme je le disais tout à l'heure, je ne suis pas très rassuré mais je ne vais quand même pas devenir parano. ***J'essaie de faire comme il faut… enfin, comme on peut aussi*** *parce qu'il faut bien travailler, voyager avec des ordi… »*

Notons, pour ce dirigeant, l'absence de mesure d'une part mais aussi les messages d'information transmis par ces proches d'autre part et qu'il ne prend pas en compte :

D3 : « Dans mon souvenir, un ami ***m'avait alerté*** *en me disant tu sais c'est vachement sensible les données, si jamais tu perds quelque chose c'est pas évident, c'est une perte sèche pour la société. …. Je n'étais pas du tout sensible à ça. Je ne suis toujours pas sensible sur le fait de dire attention, ah là là, si jamais ma société elle brûle !* ***Je n'y crois pas à ça. Ça j'y crois pas, je ne vois pas pourquoi elle brûlerait. »***

D3 : « …c'est ma faute parce que le prestataire informatique m'avait dit quand même il faudrait que tu déportes ta sauvegarde, c'est important. ***Et moi je disais de toute façon si on brûle, la sauvegarde sera dans le bâtiment alors !*** *Il m'a dit tu fais comme tu veux, moi je t'ai prévenu ! »*

5.2.5. Synthèse des risques perçus, des menaces et des conséquences

En préambule de la synthèse sur les risques perçus, les menaces et les conséquences, nous avons notés, dans les verbatims, trois champs lexicaux propres aux **émotions**, aux **sentiments** et aux **risques.** Ces champs lexicaux convergent avec les éléments considérés lorsqu'il s'agit de risque globaux :

- **Émotions : angoisse, « toucher du bois » et peur**

  *D5 : « …je crois qu'il y a **une transmission d'angoisse »***

  *D3 : « …des bâtiments qui avaient brûlé, des vols, des choses comme ça. Mais nous ça fait 40 ans… **je touche du bois** … »*

  *D12 : « …et pour le moment **je retouche du bois** parce qu'il n'y a pas de problème »*

  *D12 : « Après **je touche du bois** on a jamais eu de gros problèmes en huit ans d'existence »*

  *D6 : « Par **peur** de casser mon ordi ou de le perdre ou qu'on me le vole ».*

  *D13 : « …ça reste toujours **cette petite peur** de la concurrence qui viendrait me faire un piratage de mes données »*

- **Sentiment : sensible, paranoïa, ressenti**

  *D1 : « pour ne pas avoir qu'une seule sauvegarde du fichier auquel je suis **sensible** »*

  *D2 : « …. Je n'étais pas du tout **sensible** à ça »*

  *D3 : « Je ne suis peut-être pas **sensible** à ce discours-là » et « Je ne suis toujours pas **sensible** sur le fait de dire attention »*

  *D3 : « Je ne suis pas **quelqu'un de parano**, absolument pas et donc j'ai envie de dire pour moi ça n'avait que très peu d'importance »*

  *D4 : « … du coup je suis très **sensible** sur la sécurisation 3D »*

  *D6 : « …donc je suis plus **sensible** à l'impact du chiffre d'affaires »*

  *D14 : « Et j'ai **ressenti** le besoin de vraiment séparer les activités. »*

- **Risques : inquiétude, malheur, drame, catastrophe, accident, péril, anéantissement, et problème.**

  *D1 : « … mais plus **inquiet** d'un risque de piratage et que ces données se retrouvent dans la nature »*

D2 : « Cela fait beaucoup de si. Globalement on n'est pas vraiment ***inquiétés*** *».*

D8 : «…ça ça m'a toujours ***inquiété****… »*

D8 : « Moi ça (ransomware) ***m'inquiète****, alors peut-être un peu trop mais oui ça* ***m'inquiète****… » et « D'abord la perte de données pure et dure qui* ***m'inquiète****… »*

D9 : « Je ne vis pas dans ***l'inquiétude*** *car je me dis qu'au pire on perdrait… »*

D1 : « qui vont vous raconter une expérience ***malencontreuse*** *»*

D4 : « Mais ça ***c'est global à toutes les entreprises c'est malheureux****. »*

D9 : « Après, il y a une expérience ***malheureuse****… »*

D5 : « ***ce serait vraiment dramatique*** *effectivement de perdre des données ».*

D5 : « Je me suis dit que s'il nous arrivait la même chose ce serait assez ***catastrophique ».***

D9 : « Sinon c'est compliqué de se dire on va attendre ***l'accident*** *… »*

*D6 : « Donc si ça m'arrivait ce serait une perte de temps et la perte du travail, la p****erte totale*** *de ce qui a pu être fait entre la dernière sauvegarde* ***et le moment de l'accident*** *».*

D4 : « … si on ne sécurise pas certaines données, comme le paiement, comme la gestion avec la Douane, etc… ***on met en péril l'activité ».***

*D9 : « …****d'un schéma où il faut de temps en temps se mettre en faux péril,*** *… ».*

D1 : « Cela serait ***l'anéantissement*** *de l'ancienneté et de tout ce que ça peut apporter dans mon activité… ».*

D3 : « … on n'a pas eu de ***problème majeur*** *là-dessus, donc pourquoi ça arriverait* ***? »***

D12 : « … on a jamais eu de ***gros problèmes*** *en huit ans d'existence ».*

Nous relevons, dans les propos des répondants, l'association entre risques perçus, qu'ils soient imaginés, vécus, ou médiatisés, et la **« prise de conscience** », qu'il s'agisse d'une prise de conscience 1) sur les pertes possibles et 2) sur les menaces :

1. *D1 : « …on a tous quelqu'un qui râle parce qu'il a* ***perdu les données*** *pas forcément pro et je pense que ça fait partie de cette ambiance collective,* ***une prise de conscience*** *pour certains, … »*

D3 : « Oui. Je pense que je n'avais pas ***du tout conscience de ce que cela pouvait impliquer.*** *Quand on a été touchés* ***par le ransomware, ça nous a bloqué tout le serveur****. Par chance, l'informaticien, avait fait un truc dans le menu racine donc il y avait une sauvegarde qui se faisait dans le menu racine et le ransomware n'a pas pu aller là-dedans. Enfin c'est ce qu'il m'a expliqué car comme je vous ai dit je n'y comprends pas grand-chose, donc on a pu récupérer assez rapidement notre logiciel d'exploitation, par contre* ***on a perdu tous les fichiers qui étaient sur le serveur****. »*

D5 : « Ce dont on ***a pris conscience à ce moment-là c'est l'importance de ces données****, quand on s'est rendu compte … on a scanné pendant trois jours quelque chose qui ne s'est jamais sauvegardé …mais ça nous a fait* ***prendre conscience*** *qu'il fallait peut-être sauvegarder les données parce qu'on s'est dit que* ***si on venait à perdre des jours des jours des jours comme ça … ce serait des milliers d'heures de perdues »***

D9 : « ***…*** *se font piquer leurs données, qui perdent leur informatique, qui se font pirater leur système et qui se font demander une rançon, etc., etc… tout ça fait que l'on se dit ''****et moi, si ça m'arrivait demain, comment je gère*** *?'' »*

D11 : (au sujet du comportement de son ingénieur informatique) *« …du jour au lendemain c'est devenu une catastrophe ! Bon on s'en est séparé mais n'empêche que là j'ai vu tout le risque et là on a vraiment perdu du temps pour tout remettre d'équerre et donc là ça a été vraiment pour* ***moi une prise de conscience*** *on m'en avait déjà parlé qu'aujourd'hui le risque est quand même finalement est beaucoup plus important en interne qu'en externe. »*

D16 : « Et donc quand ***j'ai pris conscience de ça****, je me suis dit qu'il fallait protéger nos informations des risques qui pouvaient nous tomber dessus ».*

Nous notons que la perte de données et de sauvegardes sont majoritairement évoquées dans les risques perçus et également dans les conséquences des risques. Selon les répondants, la connaissance des risques est issue des risques rencontrés et également des risques communiqués, par des proches et les prestataires, et aussi par les associations, ces canaux d'information n'étant pas exclusifs l'un de l'autre.

Particulièrement aux menaces sur les SI, les verbatims évoqués par les répondants relèvent majoritairement d'une action malveillante d'un collaborateur, que cette menace se soit traduite par la survenance d'un risque (D11), ou qu'elle soit seulement envisagée (D8 ; D10 ; D12) ou du défaut de pratiques du prestataire (D3 ; D4 ; D6). Ainsi D11 évoque un

collaborateur qui *« a commencé à faire vraiment des grosses grosses conneries, à saccager une partie de nos codes sur le SVM, à saccager des éléments importants de notre informatique […] il utilisait des VPN privés depuis son poste pour pouvoir contourner notre fire-wall interne … ».* D8 se demande quelles mesures adopter pour *« pour éviter que le garçon puisse devenir potentiellement un problème demain matin »*, D10 s'est aperçu du potentiel de nuisance d'un ancien collaborateur qui « *venait sur notre système pour voir un peu ce qu'il se passait même s'il n'y travaillait plus »,* et D12 narre le départ d'un collaborateur de confiance à qui ses accès au SI sont restés actifs, qui lui a *« écrit un mail un mois après en disant ''je t'aimais pas je te supporte plus et ça fait un mois que je suis parti et j'ai encore mes accès''* ». Mentionnant les prestataires, D3 critique sa dépendance à un prestataire informatique qui ne lui permettait plus d'accéder à ses propres serveurs (« *Vous ne rentrez pas* ***sur votre serveur, enfin ça ce n'est plus possible !*** *»*), D4 évoque un prestataire unique dont il est dépendant *(« qu'on soit dépendants que d'une entrée, ça paraît complètement fou […] C'est vraiment là-dessus où on n'est pas bons ! »)*, D6 indique qu'il en est « mécontent » car il n'y avait pas de contrôle sur la sauvegarde (« *…**j'ai découvert moi par hasard**, […], que **les sauvegardes ne se faisaient plus** »).*

De l'exposition à la menace émerge aussi des verbatims de trois dirigeants. Si l'un d'entre eux (D9) évoque la nécessité de mesures préventives pour la SSI, les deux autres (D3 ; D12) estime « être à l'abri ». Ainsi, D9 évoque une analogie avec la sécurité routière pour faire valoir la nécessité de prévoir l'accident, car il est « conscient qu'on (il) n'est pas à **l'abri d'un problème…** ». D3, à l'appui de l'absence d'évènement depuis *« 40 ans »,* se questionne sur l'occurrence du risque : *« on n'a pas eu de problème majeur là-dessus, donc pourquoi ça arriverait ? ».* Il met en perspective le niveau du chiffre d'affaire de son organisation pour écarter la possibilité d'une menace sur son SI : *« Pour moi, je ne voyais pas qui pourrait nous hacker : notre société fait 1 million de CA max, on ne pèse rien. Sauf que je n'avais pas pensé au ransomware ».* Enfin si D12 *« retouche du bois parce qu'il n'y a pas de problème »,* il précise que l'absence de problème durant les 8 années d'activité de son organisation et la faible visibilité de son entreprise offrent une faible exposition aux menaces : *« on a jamais eu de gros problèmes en huit ans d'existence »* et *« …on est plutôt en mode discret donc je pense que ça joue… »*

Notons la relation directe entre **menace et incapacité à assurer le fonctionnement** de l'organisation pour D7 : *« Pourquoi une aversion au risque ? Parce que, en permanence, aujourd'hui, parce qu'on est dans une société totalement déresponsabilisée, déraisonnable. Quand un petit s'est fait mal à la tête parce qu'il a pris le poteau, ce n'est pas le petit qui n'avait*

pas de casque ou qui était au mauvais endroit, c'est le poteau qui est au mauvais endroit » (il s'agit ici de l'impossibilité d'assurer la traçabilité des actions de l'organisation et des clients, rendant impossible l'imputabilité de la potentielle faute).

S'agissant des menaces, nous relevons les propos de deux dirigeants qui soulignent une interrogation face aux menaces qu'ils perçoivent :

> *D1 : « Alors peut-être qu'effectivement l'audit qui est prévu d'être réalisé par cet ami va révéler que **je me berce d'illusions** sur la sécurité des données c'est même très vraisemblable mais en tout cas, je n'ai pas eu de consultation de quiconque sur la manière dont je protège mes données. »*
>
> *D7 : « C'est comme une maison, vous avez beau mettre un portail, toutes les protections, et bien le **pépin** il va **venir dans la faille que vous n'avait pas vue**. Je suis convaincue que vous ne pouvez voir la faille que si régulièrement **vous avez des gens de l'extérieur qui viennent regarder le truc.** »*

Les verbatims sur les menaces font aussi émerger le regard des dirigeants sur leurs **prestataires**. Ainsi :

- D3 souligne **la dépendance marquée** à la volonté de son prestataire d'intervenir sur son SI *(« Vous ne rentrez pas **sur votre serveur, enfin ça ce n'est plus possible** »)*
- D4 pointe **la dépendance à un prestataire unique** *(« et qu'on soit dépendants que d'une entrée, ça paraît complètement fou […] c'est là-dessus où on n'est pas bons ! »)*
- D6 manifeste **son mécontentement** quant au professionnalisme de son prestataire *(« j'en suis même plutôt mécontent et j'ai découvert moi par hasard […] que les sauvegardes ne se faisaient plus… »)*
- D7 **met en doute le professionnalisme** de son prestataire *(« Mais ce sur quoi je ne suis pas rassurée, c'est que j'aurais aimé faire un audit, […] de la sécurité informatique du dispositif. … Parce que je pense que mon interlocuteur raconte des c… »)*
- D8 **imagine une défaillance de son prestataire** qui pourrait le « hacker » (*« Je ne suis pas à l'abri que **mon gentil prestataire**, que je connais depuis un an, joue au casino demain et soit pris à la gorge financièrement, qu'il ait besoin de pognon et qu'il monte tout un système pour hacker tous ses clients. On n'est jamais à l'abri de cela ! »)*

Les autres verbatims sur les menaces mentionnent la perte ou le vol de matériel, l'incendie, le piratage, et dans une moindre mesure, l'environnement.

Les conséquences de la survenance d'un risque sur le SI des entreprises se traduisent en termes de poursuite de l'activité, perte de chiffre d'affaires, perte de temps, perte financière et perte d'image, situant l'ensemble de ces pertes à un niveau « métier ». Notons que ces pertes sont majoritairement exprimées par l'association à des pertes de données.

Les conséquences directes **sur la poursuite de l'activité** sont évoquées par trois dirigeants suite à la perte de données. D1 précise qu'en conséquence d'une perte totale des données, ce *« serait l'anéantissement de l'ancienneté et de tout ce que ça peut apporter dans mon activité… »*. D2 souligne l'importance de la sauvegarde sans quoi il devrait *« fermer la boutique »*.

D1 met en perspective de la perte irréversible de ses données une « *une estimation approximative »* de *« 20% »* de **perte de chiffre d'affaires***.* D2 évoque la perte de clients, impliquant 30% de CA en moins par le départ de client qui n'auraient pu être *« fidélisés ».*

Si la perte de CA est évoquée, la **perte de temps** émerge des verbatims, soit comme cause à la perte de CA soit comme conséquence directe. Nous notons que cette perte de temps peut être aussi associée à une perte de données. D5 met en perspective la perte de données d'une perte de temps durant laquelle l'activité n'a pu être assurée, causant une perte de *« trois ou quatre mois de CA »* temps qu'ils consacré « *à ne faire plus que ça c'est-à-dire que récupérer les données, ils n'ont plus travaillé »* et n'ont *« pas eu d'extension et pas de croissance ».* D3 indique le lien entre la perte de données et de temps durant lequel il a dû mettre à jour ses données et « reconstituer une base ». D5 précise que s'il perdait ses données *« ce serait des milliers d'heures de perdues »* alors que pour D6 *« ce serait une perte de temps et la perte du travail, la perte totale de ce qui a pu être fait entre la dernière sauvegarde et le moment de l'accident ».* Enfin, D16 précise *« Perdre, ça peut nous mettre dans une très mauvaise position, outre la perte de temps.*

Les **pertes financières** et **économiques** émergent elles aussi, soit comme conséquence directe, soit comme conséquence de la perte de données. Par exemple D8 précise que *« la perte d'informations qui peut mettre tout le monde au chômage »* alors que D11 met le chômage de ses salariés en perspective d'un dysfonctionnement de son SI*.* La perte financière peut aussi être mise en conséquence d'une perte de donnée, pour D13, un concurrent qui aurait « volé » ses données *« pourrait essayer de travailler avec le propriétaire,*

essayé de le contacter, essayer de le prendre en gestion » (D13) ou la conséquence d'un piratage qui pourrait provoquer la perte de *« 200 ou 300 000 € en une nuit »* (D11). La perte financière, conséquence d'une perte de donnée, est considérée comme insurmontable par D8 *« parce qu'on est super tendus depuis des années et que c'est le genre de choses qui nous coûterait trop cher ».*

La **perte de données** peut aussi avoir des répercussions au-delà de l'entreprise et se traduire par un **impact sur l'image**. D3, après avoir perdu ses élément de facturation précisé que *« quand vous devez appeler un client pour lui dire ''pouvez-vous me renvoyer votre bon de commande parce qu'on ne sait pas où il est passé'', même si vous dites on a eu un problème informatique, c'est une position embêtante ».* D4 indique « *le risque de dépréciation du service : quand un site est ralenti c'est pénible et donne une mauvaise image, quand le service client ne répond pas, on a une mauvaise image, etc, etc… »*

L'acceptation du risque apparait dans les propos des dirigeants, par la mise en œuvre de sauvegarde ou par l'absence de mesure ou. Notons que pour deux dirigeants, il est question de revoir le niveau global de sécurité avant de se prononcer sur l'acceptation.

D5 s'appuie sur la perte et le recouvrement de ses données expérimentés grâce à son système de sauvegarde pour justifier la protection de ses données *« il m'est déjà arrivé de perdre des données mais on les a récupérées facilement puisqu'on est allés puiser dans les sauvegardes… »*

Ainsi, D4 associe l'acceptation du risque à l'absence de mesure *« en fait se dit que ça peut arriver et finalement on en accepte le risque. On l'accepte puisqu'on ne fait rien pour le contrer »*, en mettant ce risque en perspective d'une potentialité faible *« on change tellement souvent que finalement, oui copiez nous mais dans 5 mois ça ne sera déjà plus ça ! […] c'est presque volontaire, ce n'est pas quelque chose sur lequel on met l'accent parce que finalement si on a accès à ces données-là, ce n'est pas très très grave ! ». D14 quant à lui s'appuie sur les informations « papier » pour écarter le risque : « …ça permet d'avoir ses papiers avec soi, de traiter ses papiers, de les copier si on a besoin, d'archiver. Avec l'informatique, on peut être soumis à des virus, des attaques, des pannes. Nous on n'est pas experts. Le papier on arrive à le gérer ! ».* Enfin pour D15 *« …le seul système de sécurité … c'était le broyeur parce qu'effectivement ces* ***numéros de CB qui se baladent c'est ''moyen''*** *».*

Enfin, D7 évoque le besoin d'être accompagné par des spécialistes pour analyser les menaces auxquels ils sont exposés : *« Mais ce sur quoi je ne suis pas rassurée, c'est que j'aurais aimé faire un audit, pas de mes procédures (elles sont déjà auditées) mais de la sécurité informatique du dispositif. ... Parce que je pense que mon interlocuteur raconte des c… »*

Les risques pour le SI, le dirigeant et l'entreprise	
Risque perçu	*« Il y a ce qu'on entend et ce qu'on a vécu. … Donc je suis assez sensible à ça, au fait que ça arrive très très vite et qu'on ne peut pas le voir venir. »* *« Mais sur Mais sur le moment, non, on n'a pas forcément imaginé tout ce que ça pouvait impliquer. »* *« Sinon c'est compliqué de se dire on va attendre l'accident pour voir si on est capable de déclencher un plan blanc. »* *« …en général quand je vois qu'il y a un petit truc qui est arrivé parce que tant qu'on ne sait pas, on fait rien. Tant qu'il ne nous est pas arrivé ou qu'il n'est pas arrivé à quelqu'un d'autre on ne l'imagine pas… »* *« Je ne sais pas, c'est purement de l'imagination. Je ne sais pas quel problème on pourrait avoir… »* *« C'est ça le risque. La violation du secret professionnel c'est ça, c'est la diffusion d'informations sensées être secrètes. »* *« Suite au crash quand j'étais étudiant… Et là c'est le vide absolu. …. J'ai perdu 3 ans de photos, de cours, travaux. Je n'avais aucune sauvegarde, rien du tout. »* *« Il y a forcément des échanges avec des gens de cercle proche ou moins proche d'ailleurs qui vont vous raconter une expérience malencontreuse »* *« … ils ont connu un problème de perte de données et donc cela m'a fait prendre conscience que cela a complètement désorganisé le cabinet »* *« Il y a nos amis avocats, en dessous, qui se sont fait pirater parce que l'une de leurs assistantes a téléchargé une recette … »* *« Il y aussi le journal télévisé où tu entends ces histoires de piratage et de demande de rançons. »* *« Les expériences des voisins, partenaires, amis qui se font piquer leurs données, qui perdent leur informatique, qui se font pirater leur système et qui se font demander une rançon, etc., etc… »*
Menace	*« Alors de piratage pas vraiment parce que d'abord je ne suis pas une multinationale et je ne pense pas être la cible numéro 1 […] ce n'est pas une banque »* *« Pour moi, je ne voyais pas qui pourrait nous hacker : notre société fait 1 Million de CA max, on ne pèse rien. Sauf que je n'avais pas*

	pensé au ransomware. » *« Parce à un moment il peut y avoir une panne sèche. Ce qu'on veut éviter c'est que quand l'avion est en l'air, il se scratche même si c'est une chance sur un million. Voilà ! »* *« Mais nous ça fait 40 ans… je touche du bois … on n'a pas eu de problème majeur là-dessus, donc pourquoi ça arriverait ? »* *« Mais il suffirait qu'il y ait un individu malintentionné qui vienne juste pour prendre le matériel ce n'est pas le matériel en soi qui me pose problème c'est ce qu'il y a dedans »* *« C'est comme une maison, vous avez beau mettre un portail, toutes les protections, et bien le pépin il va venir dans la faille que vous n'avait pas vue. Je suis convaincue que vous ne pouvez voir la faille que si régulièrement vous avez des gens de l'extérieur qui viennent regarder le truc. »* *« …que les sauvegardes ne se faisaient plus donc j'étais en roue libre au total sans savoir depuis combien de temps ça a duré… »* *« Je ne suis pas à l'abri que mon gentil prestataire, que je connais depuis un an, joue au casino demain et soit pris à la gorge financièrement, qu'il ait besoin de pognon et qu'il monte tout un système pour hacker tous ses clients. On n'est jamais à l'abri de cela ! »* *« … un de mes ingénieur qui a un moment a commencé à faire vraiment des grosses grosses conneries, à saccagé une partie de nos codes sur le SVM, à saccagé des éléments importants de notre informatique… »* *« …la personne qui est parti, on avait une totale confiance en elle et elle a pas été très clean »*
Conséquence	*« Cela serait l'anéantissement de l'ancienneté et de tout ce que ça peut apporter dans mon activité, cela veut dire reparti à zéro »* *« je dirais 30% parce que c'est ce qui doit correspondre à peu près au taux de clients qui ne sont pas fidélisés,… »* *«… je ne vais pas dire ''on ferme la boutique''. Non. Ça pourrait aller jusque-là … »* *« Je crois qu'ils ont perdu trois ou quatre mois de CA, ils ont consacré trois à quatre mois de l'année à ne faire plus que ça c'est-à-dire que*

	récupérer les données » *« … je ne sais pas. J'appellerais mon prestataire en lui demandant comment cela est possible sachant tout ce qui me coûte… »* *« Donc la perte d'informations qui peut mettre tout le monde au chômage, ça ça m'a toujours inquiété… »* *« … on va retomber sur nos pattes, on va en sortir mais ça peut être un coût de 30, 40 ou 50 K€ d'opérations en temps passé, en temps perdu à reconstituer… aujourd'hui on fait 2 M€ de CA, donc 2,5% à 3% du CA… » et « parce qu'on est super tendus depuis des années et que c'est le genre de choses qui nous coûterait trop cher. »* *« Si jamais on coupe le téléphone vient à rencontrer un dysfonctionnement les personnes sont immédiatement au chômage technique ! »* *« …et là vous vous retrouvez avec une note que vous allez devoir régler et qui peut être de 200 ou 300 000 € en une nuit, c'est énorme ! […] le risque qui est colossale parce que beaucoup de boîte ont coulé à cause de ça »*
Acceptation du risque	*« Mais ce sur quoi je ne suis pas rassurée, c'est que j'aurais aimé faire un audit, pas de mes procédures (elles sont déjà auditées) mais de la sécurité informatique du dispositif. … Parce que je pense que mon interlocuteur raconte des c… »* *« …tout brûle, tout explose… j'ai un deuxième bureau en fait, ça c'est mon bureau disons commercial et j'ai un bureau de travail… ça permet d'avoir ses papiers avec soi, de traiter ses papiers, de les copier si on a besoin, d'archiver. Avec l'informatique, on peut être soumis à des virus, des attaques, des pannes. Nous on n'est pas experts »* *« …le seul système de sécurité que j'ai mis en place à un moment, vraiment c'était basique, c'était le broyeur parce qu'effectivement ces numéros de CB qui se baladent c'est ''moyen'' ». »*

Tableau 15 : Synthèse des verbatims sur les risques pour le SI, le dirigeant et l'entreprise

5.3. Influences isomorphiques

Les influences isomorphiques, normatives, coercitives et mimétiques, sont associées aux verbatims qui révèlent respectivement les effets des réseaux, de professionnels ou associatif, voire de proche, les effets de la loi ou de la réglementation et les effets de l'adoption des pratiques d'un concurrent.

5.3.1. Influences normatives

Les influences normatives qui sont précisées, pour les dirigeants interviewés, reposent sur les pratiques professionnelles répondant à de possibles mises en cause (D7 et D9) ou au manque de connaissance appelant à se renseigner auprès de professionnels.

> *D7 :* (précisant le besoin de sécurité de son SI et des décisions formelles dont il conserve la trace) *« **Personne n'assume rien** ! Donc quand on prend un prestataire comme nous, la première réaction maintenant qu'ont les gens c'est ''je prends un expert-comptable et s'il se trompe, ce n'est pas ma faute '' […] On est de plus en plus dans une judiciarisation de la Société, à mon avis de plus en plus conflictuelle et nous, en permanence on se méfie, on redemande, on re-redemande ''Vous m'avez bien dit que ? J'ai bien dit que ? On est bien d'accord que ? Et malgré cela : '' je ne comprends pas, **vous ne me l'avez pas demandé** !'' »*
>
> *D9 : « …si on ne conserve pas **la justification et qu'après on a une remise en cause** par le client parce que ses intérêts ont changé, parce que ça l'arrange de dire l'inverse, ou je ne sais quoi d'autre, et bien il nous faudra faire la preuve que ce qu'on a fait, on l'a fait avec lui, par lui et par ses instructions »*
>
> *D13 : « Honnêtement je n'ai pas trop de recul. **Je n'avais pas trop de vision là-dessus** je me suis **un petit peu renseigné j'ai écouté des gens autour** j'ai fait **confiance à des professionnels de l'informatique** qui sont venus m'installer mes systèmes alors que moi j'y connaissais absolument rien au niveau informatique donc même si j'aime bien je n'ai pas les connaissances mais j'ai fait confiance aux personnes qui étaient là donc il y a eu des choses bien, des choses moins bien »*
>
> *D8 : « Mais la sécurité, enfin les postes informatiques en eux-mêmes, j'ai dans mon historique, **mon premier prestataire qui est toujours là régulièrement**, […] et qui a*

été mon tout premier prestataire en 2000 quand j'ai commencé à avoir les premiers postes informatiques pour les installations, les nettoyages, les anti-virus etc... Même encore aujourd'hui, quand j'ai ***des besoins un peu spécifiques, ça m'arrive encore de l'appeler plus lui que mon prestataire actuel****. Au moindre truc peut-être un peu plus sensible, réflexe, c'est lui que j'appelle ! »* et de compléter *« il est très pédagogue, a toujours fait attention à me dire tout ce qu'il faisait et pourquoi il le faisait et aujourd'hui j'arrive à tripatouiller un certain nombre de trucs en informatique que* ***j'ai appris uniquement à ses côtés****, en écoutant ce qu'il faisait. Donc il m'a appris pas mal de choses et m'a toujours alerté sur plein de trucs. Donc je pense que dès 2000-2001, quand il a commencé à s'occuper de la gestion informatique, ça l'a préoccupé. »*

D17 : « comme je disais tout à l'heure, c'est une prise de conscience progressive. On progresse, on regarde les autres, on écoute et on finit par s'adapter »

Notons que les mesures partagées par le professionnel (prestataire de confiance en l'occurrence) peuvent être mises en œuvre directement par ce dernier (D8) *: « Je pense que c'est lui, parce que* ***j'ai confiance*** *dans ce qu'il me dit et dans ce qu'il fait et que s'il* ***me dit que c'est important et qu'il faut le suivre****, je ne me suis* ***pas trop posé de questions en fai****t. Tout ce qu'il a fait a toujours été très bien fait. À partir du moment où on a confiance en quelqu'un et que mec dit on ne se prive pas d'antivirus, on ne se prive pas d'installations sécurisées, on met des mots de passe Wi-Fi plus longs, je ne me* ***suis jamais posé de questions, je l'ai toujours laissé faire****. Après il aurait peut-être pu faire mieux aussi mais je pense qu'il a fait ce qu'il aurait fait dans sa propre boîte. »*

5.3.2. Influences coercitives

On note dans les influences coercitives la réglementation sur la protection des données, issue de la CNIL ou du RGPD (Règlement général sur la protection des données) ou encore d'une règlementation particulière

Ainsi D1 souligne la connaissance et la volonté de répondre aux exigences de la CNIL, tout en indiquant, que si la menace de sanction est avérée en cas de manquement, il pense qu'elle est peu probable :*« …je pense que ça fait partie de cette ambiance collective, une prise de conscience pour certains, après non des obligations j'en ai peu, enfin la RGDP un bon exemple enfin je trouve parce que c'est quelque chose dont on parle que maintenant et cela fait longtemps qu'on sait que ça va arriver moi je* ***suis un peu plus sensible sur le sujet*** *enfin je sais pas si c'est intéressant d'en parler j'ai un très très bon ami qui travaille dans la sécurité*

informatique et qui a une offre RGPD et malgré tout moi je suis très sceptique sur la manière dont les entreprises vont toutes passer sur cette norme parce que pour moi si il y a juste une menace de sanctions mais ***qu'il y'a pas de sanction appliquée*** *».*

À l'inverse, D5 et D10 mettent en avant le cout de la sanction en cas de contrôle sur ce point de la réglementation :

> *D5 : « …on est soumis à une réglementation un petit peu particulière qui concerne la* ***protection des données médicales*** *» … « si dans le cas des assurances ils découvrent lors* ***d'un contrôle des questionnaires de santé il y a une amende par questionnaire*** *; nous à un moment donné on les a recensé on a 900 questionnaires de santé* ***et l'amende peut aller jusqu'à 150 € par dossier »***
>
> *D10* ***: «*** *Il y a un* ***risque financier****, il y a un risque de réputation les risques sont multiples vous avez vu le RGPD sur le plan financier 4 % de notre chiffre d'affaire en cas de non-respect de la règle c'est énorme très clairement et aussi un risque pénal nos patients peuvent nous attaquer si on n'a pas fait en sorte d'assurer la confidentialité de leurs données, les risques sont multiples… »*

D4 souligne l'importance de la pression réglementaire qui représente une influence marquée et nécessaire : « …je sais qu'**il y a la fameuse loi RGPD.** Donc nous, au sein de l'entreprise, **on est sensibilisés à ça auprès de nos clients et on doit rentrer dans les clous**.[…] Là encore, je pense que dès que la législation entre en jeu, c'est là où on **est les plus sécurisés** parce que finalement on **nous impose de telles lois que la sécurisation** -et là notamment je parle des factures etc…- notre expert-comptable vous dirait ça mieux que moi- mais on ne doit pas pouvoir modifier une facture, chacune doit avoir un numéro unique, qui se suit, etc…. ». D13, quant à lui, imagine un des effets du RGPD tout en soulignant la difficulté de l'appliquer : *« on pourrait avoir un client qui viennent nous voir au bout de six mois et qu'il me dise ''vous avez gardé des données à moi, je vous ai envoyé un mail comme quoi il fallait les supprimer et vous ne les avez pas effacées'' et je pense que dans les années à venir c'est là-dessus qu'on va* ***avoir des problèmes et*** *c'est pour ça qu'il faut les maîtriser mais c'est difficile pour les commerciaux parce que si c'est leur base de données de travail donc ça m'arrive de voir des mails passer où les gens disaient ''je vous ai demandé de ne plus me solliciter et d'effacer mes données'' alors qu'eux c'est leur boulot, c'est pour ça qu'il faut leur dire trois fois qu'on en veut plus avant qu'ils arrêtent… ce sont des approches différentes ».*

Si pour D7 et D9, les influences normatives sont très proches des influences coercitives, les règles issues de professions règlementées sont traduites aussi par D10 :

> *D7 : « Mais je fais des sauvegardes à tous les niveaux. Parce qu'il* ***y a des responsabilités civiles déjà,*** *pendant 10 ans, parce qu'un salaire* ***doit pouvoir être communiqué pendant 30 ans****. »*
>
> *D9 : « …mais dans l'idée, le secret professionnel* ***nous oblige à protéger nos données****, sécuriser les entrants, sécuriser les sortants et sécuriser notre travail et d'un autre côté, le risque d'un jour d'avoir à prouver ce qu'on a fait, pourquoi on l'a fait, dans quel cadre et sur quelles instructions on l'a fait****, nous oblige aussi à sécuriser les mêmes données** ».*
>
> *D10 : « sur un certain nombre de champs, notamment le c****hamp médical on est obligé de sécuriser les informations pour des raisons de confidentialité, pour des raisons de sécurité stricte*** *[…] un certain nombre* ***d'obligation*** *avec un calendrier à respecter, hôpital numérique, les* ***instructions relatives à la sécurité des SI avec trois grands pans*** *et l'obligation d'être dans les clous sur ces différents pans à l'horizon 2018 […] …je pense que les établissements de santé risquent d'avoir des* ***contrôles plus rapidement*** *que les autres puisque le milieu médical a forcément des données sensibles et extrêmement critiques et* ***on a besoin de bien maitriser notre sujet »***

D16 évoque la dualité de la protection des données, selon le risque vécu et la nécessité de répondre à la réglementation : *« Certains l'ont fait pour protéger leurs données nominatives et parce que la loi l'exigeait et d'autres parce qu'ils ont eu un vrai problème ! »*

D15 connait la règlementation sur le service de Wi-Fi offert mais n'en tient pas compte : *« …normalement, on devrait* ***pouvoir tracer*** *qui s'est connecté, à quelle heure et sur quel site.* ***Moi je n'ai pas tout cet historique-là*** *».* Notons que les échanges avec D15, alors qu'un client venait lui indiquer son impossibilité à se connecter au hotspot, ont mis en évidence une pratique illégale sur la mise à disposition d'Internet dans son établissement : *« … en fait j'ai un hotspot, enfin des hotspots, un par étage et on passe par une interface et les clients sont obligés de s'identifier avec des codes, parce que là aussi, normalement, on devrait pouvoir tracer qui s'est connecté, à quelle heure et sur quel site. Moi je n'ai pas tout cet historique-là,*

par contre j'ai l'adresse MAC de chaque appareil qui s'est connecté. » Après lui avoir demandé si cette pratique correspondait à la réglementation[67] il a répondu *« Euh... Moi je le fais surtout pour faire en sorte que je ne donne pas ma clé WEP toutes les 5'. Pareil, c'est du pifomètre. Après je me dis que je ne risque pas grand-chose avec le brave monsieur là mais voilà.* »

D16 s'appuie sur sa connaissance de l'évolution de la loi : *« Et j'ai aussi vu les évolutions au niveau des lois. Et surtout, je vois qu'aujourd'hui tout le monde diffuse tout ce qui lui tombe sous la main et donc qu'il faut faire de plus en plus attention à ce que nous faisons avec nos informations. »*

5.3.3. Influences mimétiques

Les verbatims mettent en évidence, pour D1 une pratique héritée de son père, pour D6 à la fois une pratique mimétique et un manque de connaissance des pratiques des concurrents et D7 s'inscrit dans le prolongement du dirigeant précédent :

> *D1 : « Je prends **l'exemple de mon papa** qui faisait des sauvegardes fréquentes de ses photos peut-être aussi je me rappelle avoir évoqué la dégradation du CD-ROM avec la fragilité du support en question […] quand on se renseigne quand on regarde la durée de vie, je me souviens de l'article que j'ai lu dans Sciences et Avenir qui disait que au-delà de l'obsolescence du CD, il avait de toute façon une capacité de **perte de mémoire dans le temps** ou de toute façon à partir de CD-ROM on n**e restituera pas dans son temps les données** avec des copies exploitables… »*
>
> *D6 : « …je ne savais **pas à quoi cela servait, mais pour avoir un antivirus comme tout le monde** alors je prenais des versions gratuites, jusqu'à maintenant j'ai la chance… »*
>
> *D6 : « **Je ne connais pas de concurrents** je vis tout seul dans mon coin non mais c'est vrai je ne connais pas les concurrents, aucune idée de mes fournisseurs je vis **tout seul sur mon île**… »*

[67] Art. L.32 du code de l'ARCEP, Autorité de Régulation des Communications Electroniques et des Postes

D7 : (au sujet de la protection des données et des services) *« Mon prédécesseur faisait déjà très attention »*

D16 : « Certains (partenaires, fournisseurs ou concurrents) *l'ont fait pour protéger leurs données nominatives et parce que la loi l'exigeait et d'autres parce qu'ils ont eu un vrai problème ! »*

5.3.4. Synthèse des influences isomorphiques

Les influences normatives et coercitives se rejoignent pour certaines professions réglementées. La protection des données personnelles, ou médicales, est majoritairement évoquée par les dirigeants. Ainsi, certains sont enclins au respect de ces influences, y voyant un avantage dans leurs pratiques professionnelles et en regard de leurs responsabilités, les conduisant à mettre en œuvre la protection de leurs données. D'autres y voient davantage le cout liés à la sanction en cas de non-respect. L'influence mimétique n'est que peu évoquée, sinon pour D1 qui reproduit les principes de sauvegarde de son père et pour D6 qui a mis en place une pratique pour faire *« comme tout le monde ».*

Influences normatives	*« …si on ne conserve pas la justification et qu'après on a **une remise en cause par le client** parce que ses intérêts ont changé, parce que ça l'arrange de dire l'inverse, ou je ne sais quoi d'autre, et bien il **nous faudra faire la preuve que ce qu'on a fait**, on l'a fait avec lui, par lui et par ses instructions »* *« il est très pédagogue, a toujours fait attention à me dire tout ce qu'il faisait et pourquoi il le faisait et aujourd'hui j'arrive à tripatouiller un certain nombre de trucs en informatique que **j'ai appris uniquement à ses côtés**, en écoutant ce qu'il faisait. Donc il m'a appris pas mal de choses et m'a toujours alerté sur plein de trucs »* *« Je n'avais pas trop de vision là-dessus **je me suis un petit peu renseigné j'ai écouté des gens autour j'ai fait confiance à des professionnels** de l'informatique qui sont venus m'installer mes systèmes … j'ai fait confiance aux personnes qui étaient là donc il y a eu des choses bien, des choses moins bien »*
Influences coercitives	*« … la **RGDP** un bon exemple enfin je trouve parce que c'est quelque chose dont on parle que maintenant et cela fait longtemps qu'on sait que ça va arriver… »* *« …on est soumis à une **réglementation** un petit peu particulière qui concerne la protection des données médicales » …* *« …je sais qu'il y a la fameuse loi **RGPD**. Donc nous, au sein de l'entreprise, on est sensibilisés à ça auprès de nos clients et on doit rentrer dans les clous. »* *« Parce qu'il y a des **responsabilités civiles** déjà, pendant 10 ans, parce qu'un salaire doit pouvoir être communiqué pendant 30 ans. »* *« …mais dans l'idée, le **secret professionnel nous oblige** à protéger nos données… »* *« …sur un certain nombre de champs, notamment **le champ médical on est obligé** de sécuriser les informations pour des raisons de confidentialité, pour des raisons de sécurité stricte »* *D15 « …normalement, on devrait pouvoir **tracer qui s'est connecté**, à quelle heure et sur quel site. »*

Influences mimétique	*« Je prends **l'exemple de mon papa** qui faisait des sauvegardes fréquentes de ses photos* *« …je ne savais pas à quoi cela servait, mais pour avoir un antivirus **comme tout le monde** »* *« Mon prédécesseur faisait déjà très attention »*

Tableau 16 : Synthèse des verbatims sur les influences isomorphiques

5.4. Éléments du processus de décision d'adoption symbolique

5.4.1. Perception des besoins

Il s'agit d'identifier les verbatims qui ont alimenté la réflexion sur les besoins en SSI. Les besoins exprimés relèvent le regard des dirigeants sur la survenance du risque et/ ou de ses conséquences. Ainsi, nous présentons la perception des besoins en distinguant les risques de la SSI selon qu'ils soient mis en perspective des connaissances propres au dirigeant, de l'influence de proche ou de la réglementation

- **Besoin de la SSI établi sur des pertes de disponibilité ou de confidentialité des données ou des services**

  D1, D3, D5, D10, D15 évoquent un ou plusieurs **risques vécus** engageant **une perte de disponibilité ou de confidentialité** auxquelles ils associent leur réflexion sur la SSI :

  *D1 : « Par **rapport à mon expérience**, … **mais oui victime à l'époque des CD beaucoup** ; si j'essaye de faire une prospective c'est vrai que les CDs étaient quand même un **support assez fragile** finalement peut-être plus que les disquettes même si j'ai moins bien connu cette période où **j'ai perdu des photos qui étaient sur le CD »***

  *D3 : « …bon **on a quand même pris un ransomware** ! …plus en termes de sauvegarde des données pour ne pas être embêtés ou du moins l**e moins possible en cas de rebelote sur des ransomware ou des choses comme ça**. Donc en fait j'ai un NAS, j'en ai un autre chez moi et puis Etienne tous les vendredis fait la sauvegarde complète en plus parce que du coup on a redonné un peu plus d'attention. »*

  *D5 : « Ce dont on **a pris conscience à ce moment-là c'est l'importance de ces données**, quand on s'est rendu compte … on a scanné pendant trois jours quelque chose qui ne s'est jamais sauvegardé …mais ça nous a fait **prendre conscience** qu'il fallait peut-être sauvegarder les données parce qu'on s'est dit que **si on venait à perdre des jours des jours des jours comme ça … ce serait des milliers d'heures de perdues »***

D10 : « …depuis un véhicule des gars avaient ***piraté le Wi-Fi*** *et étaient rentrés dans notre SI administratif … et en fait, avaient* ***récupéré des données qui était dans ce SI*** *[…] je sais pas comment il s'était débrouiller mais ils étaient rentrés dans le système informatique et en fait* ***avait récupéré des données*** *qui était dans ce SI parce qu'à l'époque le dossier patient n'était pas informatisé en 2008 dans le dossier administratif, il y a* ***des données nominatives de patient*** *»*

D10 : (évoquant un administrateur qui ne faisait plus partie de l'entreprise) *« … il venait sur notre système pour voir* ***un peu ce qu'il se passait même s'il n'y travaillait plus****, entre parenthèses il s'est fait virer par son nouvel employeur suite, justement, à des failles qui ont été pointées du doigt, avec des mises en garde préalables et malheureusement il s'est fait licencié »*

D15 : « … ***on est méfiant****. On entend parler de trucs, de fraudes à la carte bancaire. Enfin moi je ne suis pas très méfiant.* ***Je fais attention mais je ne suis pas paranoïaque****. Je me suis fait piquer mes papiers, ma carte bancaire, fait débiter de plusieurs milliers d'euro... pendant 8-15 jours on transpire un peu quoi. »*

D16 : « En fait, j'ai peur des virus, du pillage mais j'ai surtout peur d'un crash puisque ***j'ai déjà eu il y a quelques années dans une autre*** *structure un problème de ce style. »*

Les verbatims font aussi émerger **des risques imaginés, pouvant engager une perte de disponibilité ou une perte de confidentialité** :

D2 : « De ce qu'on entend sur le papier sorti de la poubelle qui se retrouve par terre, la facture du client qui traîne dans la rue et un document qui n'a pas à traîner là, une poubelle qui a été éventrée, ***un document qui ne m'appartient pas et que pour une raison x ou y, je suis vraiment désolé****…* ***sans parler de malveillance****. Une facture il n'y a rien de confidentiel mais je considère que ce sont des documents sensibles, comptables, qui n'ont pas forcément à traîner dans la rue. Donc c'est vraiment plus pour le client encore une fois que je détruis ce style de documents pour dire il ne sera pas dans la poubelle en tous cas, voire je le déchire en 4 minimum. »*

D6 : « Je fais partie d'un club où il y a régulièrement des gens qui ***informent les autres*** *sur les risques et voilà … »*

*D8 : « Ce qui **me pousse à sécuriser** ce n'est pas la peur de la concurrence ou de l'intrusion et de la récupération de données. Clairement moi ce qui m'a toujours inquiété c'est qu'est-ce qu'on fait si on n'a plus de poste informatique ? D'abord la **perte de données pure** et dure qui m'inquiète parce que si on n'a pas assez de back-up et que tout brûle au même endroit, tu as beau avoir 4 sauvegardes, si tu n'en as pas une sur un site distant, ça ne sert à rien. **Donc la perte d'informations** qui peut mettre tout le monde au chômage, ça **ça m'a toujours inquiété** et le temps passé à remettre un système. Là je ne parle pas d'un bâtiment brûlé mais d'un serveur qui se fout en vrac. Si tout le monde est connecté au serveur et n'a pas de données, si on est bloqués même une journée pour moi c'est une journée de trop. »*

*D10 : « Mon père effectivement étant policier m'a toujours transmis de toujours faire attention… **j'ai un tempérament un petit peu suspicieux**… […] …je me dis on peut avoir accès à beaucoup de choses, accès à notre informatique de gestion et à notre informatique médicale et à partir du moment où tout ça va être imbriqué je vais pouvoir peut-être aller choper ces **informations extrêmement sensibles**. »*

D10 : (évoquant le responsable des SI) *« Il **nous mettait en danger** à l'instant T, mais aussi pour le futur puisqu'il ne voyait pas arriver ce qui allait se passer : ces **interconnexions qui allaient monter crescendo, ces failles systèmes diverses et variées..** »*

*D13 : « … c'est parce que je **n'y pensais pas** mais on était beaucoup moins et c'était moi qui gérais tout avec mon ordinateur perso il y avait moins de personnes qui touchaient aussi à tout ça. Alors que **du coup aujourd'hui** la mauvaise manipulation d'une personne peut **tout vous effacer** donc que **je veux être aussi assuré de cela par rapport à la multiplication des personnes** qui peuvent toucher ces données et donc c'est important d'avoir des sauvegardes »*

*D14 : « **À moins que ça brûle** mais voyez j'ai une armoire ignifugée. **Alors bien-sûr si tout brûle, tout explose.** Mais j'ai un deuxième bureau en fait, ça c'est mon bureau disons commercial et j'ai un bureau de travail. J'ai séparé mes 2 bureaux. »*

*D16 : « …on peut **perdre beaucoup** en une minute si on se fait voler un ordi, des informations ou si on a un virus ou une attaque mais on n'y pense pas tous les jours quand même. **On essaie de faire attention et j'en parle souvent à mes***

***salariés**. »* et *« C'est surtout la **divulgation d'information** et les **''bêtes'' pertes d'information,** par dégradation d'un ordi, perte d'un matériel, qui m'inquiète. »*

*D17 : « C'est important de mettre en place la SSI mais je vous l'ai déjà dit, on n'avait pas trop le choix en termes de fonctionnent car **il faut bien gérer les données de tous nos clients, ne pas les égarer pour répondre à leurs demandes, à leurs nouveaux projets**, ne pas confondre un interlocuteur avec un autre et faire la mauvaise réponse à une personne ou se tromper de personne même «*

- **Besoin établi sur la SSI directement, sur la base des connaissances propre au dirigeant, des connaissances partagées avec les membres de son réseau d'influence** ou encore la nécessité de se conformer à la **réglementation**

*D4 : « C'est assez étrange d'ailleurs **ces problèmes de sécurité** parce qu'en fait on est sensibilisé **au niveau personnel**, et on s'aperçoit finalement que dans toutes les entreprises que j'ai pu voir en fait elles sont moins bien sécurisées que nos propres données personnelles. »*

*D7 : « Bon déjà le système d'information, il faut savoir que la donnée et l'information, c'est […] au cœur de notre dispositif, un élément vital de la vie de mon entreprise. […] **personnellement, j'agis par le management de la qualité** donc j'ai normé ISO mon cabinet en 2004, donc il y a déjà 14 ans. C'**est ma manière de manager la donnée dans mon cabinet**, c'est-à-dire que normalement, je dis bien normalement, la manière dont on traite les données n'est pas faite au hasard. C'est la **manière dont on récupère l'information, la manière dont elle est traitée, dont elle est rangée, dont elle est classée, la manière dont elle est conservée,** etc… »*

*D6 : « On avait Avast antivirus gratuit et ça c'est toujours bien passé […], **je ne savais pas à quoi cela servait**, mais pour avoir un antivirus comme tout le monde et que je n'avais pas d'argent pour payer ni Norton… alors je prenais des versions gratuites, jusqu'à maintenant j'ai de la chance… […]… **je faisais de la sauvegarde** des fichiers stratégiques en ligne ou des sauvegardes sur disques externes… on a que des portables quasiment alors de temps en temps on fait des sauvegardes. »*

*D16 : « Comme je n'ai pas trop de temps et de ressources, j'essaie **surtout d'écouter les mauvaises histoires des autres** et de m'y' **adapter en interne***

pour éviter les même problèmes et les mêmes conséquences ! Enfin, ça c'est l'idée parce que après faut le temps et les moyens de le faire. »

Pour D1, D5 et D9, le besoin de prendre en compte les exigences de la réglementation alimente leur réflexion sur la SSI.

D1 : « En 2009, au moment où j'ai créé ma société, ils (la CNIL) *m'ont envoyé un mail, [...] ils m'ont demandé la base de données vierge pour savoir* ***quel type de données*** *j'allais collecter et utiliser… je pense que c'est facultatif ils m'ont demandé si ça me dérangeait de le faire j'ai dit non et* ***j'a****i* ***eu un numéro d'agrément*** *sachant que cette base de données depuis 2009 a beaucoup évolué depuis mais on m'a jamais rien redemandé et* ***j'ai toujours mon agrément ad vitam aeternam*** *(rire) »*

D5 : « En fait lorsqu'on ***devient courtier, on est obligés de tout sauvegarder*** *parce que les compagnies n'ont plus le même fonctionnement qu'avec ses agents. En tant qu'agent, les compagnies sont responsables de ses actes ; un courtier c'est lui qui est responsables, donc la compagnie, en fait, ne se moque pas de la protection des données d'un courtier mais c'est secondaire ce n'est pas son problème… »*

D9 : « Non, non. Je ne me suis ***pas réveillé un matin*** *en me disant qu'il fallait faire quelque chose.* ***C'est un long cheminement****.* ***C'est des rencontres, des discussions, des expériences malheureuses de confrères ou de clients.*** *»* et *« Ce qui* ***alimente la réflexion****, ce sont plusieurs piliers. Le premier c'est le* ***secret professionnel*** *qui fait qu'effectivement on doit avoir une notion de l'information qu'on protège, qu'on sécurise, qu'on ne divulgue pas, etc... Le deuxième* ***c'est la protection face à une mise en responsabilité,*** *c'est-à-dire c'est le fait de conserver des données qui ont permis de mettre en place des situations, mise en place que l'on pourrait nous reprocher ensuite si on n'arrivait pas à justifier des données correspondantes. »*

Pour D16, la réputation est soulignée : *« En fait, nos auditeurs, ceux qui suivent nos formations, c'est notre capital, notre business et donc on peut se permettre de laisser passer des données à l'extérieur ou n'importe où sur internent. C'est* ***notre réputation*** *! »*

5.4.2. Renseignement sur la solution

Après que le besoin ait été identifié par les dirigeants, il s'agit alors pour eux de s'informer sur la façon dont la SSI peut répondre à leur nécessité de gérer le risque ou, dit autrement, d'étudier la solution permettant de protéger leur SI et ainsi éviter les conséquences défavorables liés à un incident. Pour cette phase de l'adoption symbolique nous nous attachons à présenter les verbatims qui font émerger l'origine des renseignements considérés, adossée à des connaissances personnelles, des connaissances partagées par des réseaux d'influence ou encore des connaissances acquises auprès de prestataires.

- **Renseignements basés sur des connaissances personnelles**

  *D1 : « Alors oui je suis un passionné **de nouvelles technologies** mais ce n'est pas forcément le bon terme car c'est plus un hobby, un loisir, **qu'une passion** que j'ai régulièrement mais j'aime bien être au courant de ce qui se fait, de ce qui existe dans plein de domaines y compris dans des domaines qui ne me concernent pas directement donc l'usage de l'outil informatique est un intérêt… »*

  *D1 : « … le coté informatique m'intéresse à titre personnel donc je **ne suis pas démuni lorsqu'on me dit il faut sauvegarder je sais ce que ça veut dire**, je sais comment le faire je sais où le faire. »*

  *D1 : « En fait il s'agit **d'une simple copie finalement**, qu'on pourrait **comparer à une photocopie dans le monde analogique**… L'inconvénient d'être photocopié tous les jours pour avoir aucune perte c'est de photographier une fois par semaine ou tous les 15 jours, avec une perte de données sur quelques jours de travail, ce qui est toujours embêtant dans un monde parfait, mais pas catastrophique en terme de conséquences à l'échelle de l'activité qui m'amène à reparler de cette histoire de probabilité statistique comme il y a un côté obligatoire à l'assurance automobile ce qu'il n'empêche pas de dire que il n'y aura jamais un accident... »*

  *D2 : Quand on travaille dans ce qui s'appelle maintenant « industrie d'hélicoptères militaire », on est **forcément confronté à un cadre assez sécurisé**. »*

  *D5 : (à la question d'où tenez-vous cette connaissance ?) : « c'était mon métier ! En fait j'étais inspecteur chargé de **contrôler, de former de diriger les courtiers**, donc je connaissais ça au quotidien **de mettre en garde** aussi sur le plan juridique sur le plan fiscal, **sur le plan des données**… »*

D6 : (sur l'origine de ses connaissances techniques poussées : virtualisation, VPN, RAID,…) *« **De moi** ! **Je n'ai pas de connaissances mais je suis à l'ancienne** alors que le cloud n'existait pas il y a 10 ans, je vous le rappelle, et donc j'ai grandi avec des disques durs et des disquettes molles et **j'ai gardé mes habitudes de mes disques durs auprès de moi pour faire des sauvegardes….** […] De toute façon avec ma **vieille mentalité** je préfère **avoir un bon serveur ici que physiquement que je vois** et j'ai **l'impression que mes données sont là** plutôt que quelque part perdu sur l'Internet. »*

*D9 : « …j'ai effectué mon service militaire je le fais dans la transmission… donc je suis habilité et on est **sensibilisés à ces questions**-là… »*

*D11 : « … **j'étais dans la partie informatique** enfin quand on fait la physique on fait beaucoup de théorie et de modélisation tout passe par des gros calculateurs les fameux ''**grid''** et ensuite en tant que chercheur même si on peut avoir le support de techniciens informatiques, **on doit être capable de maîtriser les capacités** pour faire du calcul en parallèle sur plusieurs machines...»*

*D14 : « Moi je suis un garçon **qui lit pas mal**, donc lire, parler avec des gens, voir comment ils fonctionnent et peut-être aussi à l'armée où j'ai **appris des façons de de faire.** Ça s'est fait comme ça, de façon empirique. »*

D16 : « La sécurité chez Sun était très importante. Nous avions des formations et des outils pour gérer la SSI » et *« J'ai eu pas **mal de connaissances et même des formations dans mes précédents boulots**. »*

- **Renseignements basés sur des connaissances partagées par des réseaux d'influence**

  D2 : « …j'ai eu l'intervention d'un professeur de la DST, un vacataire en fait, lors de ma formation, qui nous a sensibilisés à la sécurité mais pas tant informatique mais plutôt aux entretiens, à la façon dont on peut se faire cuisiner discrètement pour avoir des informations, surtout quand on était dans des jobs un peu sensibles. »

  *D3 : « Alors, **j'ai eu un copain qui a 3 ou 4 sociétés** je crois et qui m'a dit ''moi je me suis libéré de tout ça. Je suis sur Google et je ne m'embête plus la vie. J**e maîtrise tout''**. Il m'a montré son téléphone en me disant ''si je veux changer mon mot de passe je le fais de là, je gère tout de là et j'ai viré toutes les sociétés informatiques et au final je m'y retrouve''. »* et *« J'ai des amis qui disent ça : tu vois, ça risque pas d'arriver à Google,*

c'est impossible et même s'ils se font pirater, il y a tellement de sauvegardes, de sauvegardes, de sauvegardes, que tes données de toute façon tu les récupères, il n'y a aucun problème »

*D8 : « Il **y a plein de clubs** … donc c'est des réunions 1 fois par mois, avec des consultants et des intervenants qui viennent **sur des thématiques spécifiques** ».*

*D9 : (sur la question de l'origine de ses connaissances) « Je **ne sais pas : c'est la TV, c'est un ami spécialiste en sécurité, c'est le bon sens…** »*

*D13 : « …parce qu'autour de moi j'ai des **particuliers et des professionnels** […] je me dis que **l'expérience de quelqu'un va me servir à moi** c'est pour ça que c'est fait je pense… et du coup lui il a eu ça moi je vais vérifier ce que j'ai et je regarde si c'est bon ou si ça peut m'arriver aussi donc à ce moment-là je me renseigne […] et **on peut voir si on peut mettre ça ou ça en place**. »*

*D11 : « Quand j'ai monté l'entreprise, […] je suis rentré dans un centre de formation pour la création d'entreprise, et là-dedans ils ont fait intervenir un **consultant de la DST** qui nous a parlé de la sécurité justement dans les grandes lignes. Son grand jeu était de prendre le TGV et quand quelqu'un partait s'acheter une bricole, à boire ou autre chose, soit il allait piquer son PC soit il allait y faire quelque chose dessus pour montrer son accessibilité… et surtout quand il se rendait compte que c'était de grandes entreprises regardait comment il se comportait et allait leur en parler pour les sensibiliser… et c'est vrai que ce discours de dire que la sécurité et notamment dans les TPE/PME, n'est vraiment pas pris en compte… »*

*D14 : « Oui, quand on se **rencontre au syndicat, on discute.** Eux nous font remonter des **informations, des alerte**s… C'est assez actif, on a un très bon syndicat : il fait de la veille réglementaire, de la veille commerciale. Cela **fait un ensemble d'outils grâce auquel on peut lire, voir ce qu'on avoir, ce qu'on échange**. »*

*D16 : « J'écoute aussi beaucoup les **personnes avec qui je travaille**. Enfin, surtout ceux de l'extérieur »*

D17 : « J'ai aussi plusieurs amis qui m'ont donné pas mal d'informations et de contacts pour mettre en place des procédures de sécurité »

- **Renseignements basés sur des connaissances acquises auprès de prestataires**

*D3 : « …**notre fournisseur** avait compris que ça ne servait à rien de pousser, qu'il fallait que **je sois prêt à entendre le discours. Je ne l'étais pas franchement, du tout. Pas du tout..** »*

*D6 : « **Oui je suis conseillé par un prestataire** depuis qu'on a installé un ERP, il y a trois ans ».*

*D8 : « De sécurité d'une manière générale parce que d'abord ils sont aussi très accros à la sécurité, donc les virus, les mises à jour des antivirus, le nettoyage permanent des PC, la vérification des spams, c'est toujours quelque chose **qui l'a préoccupé*** (le prestataire) *»*

*D8 : « j'ai confiance dans ce **qu'il me dit et dans ce qu'il fait et que s'il me dit que c'est important et qu'il faut le suivre, je ne me suis pas trop posé de questions en fait…** »*

*D13 : « … On a fait ça avec **mon informaticienne qui me disait ça c'est bien ou ça ça suffit** par rapport à ta capacité, par rapport à ce que tu as, par rapport à ce que tu veux faire il n'y a pas la nécessité de plus mais il n'y a urgence à travailler là-dessus si un jour il y a un besoin de plus on mettra quelque chose de plus costaud en place mais là, pour l'instant T, ça suffit... »*

*D13 : « L'informaticienne était plus dans l'optique d'une sauvegarde des données dans le cadre d'un disque dur qui crame ou un truc comme ça **c'est plus son idée au départ plus la perte de données que du piratage** et en cas de disque dur qui crame et où on perdrait toutes nos données que ce soient les mails et tout ça… »*

D13 : « Elle (l'informaticienne) *a été un petit peu plus dans la **minimisation des risques** plutôt que de mettre en perspective les potentiels problèmes qu'il pourrait y avoir, souvent elle disait qu'il y avait des choses dont on n'avait pas besoin en précisant qu'avant qu'il arrive ça ou ça ou que tu te fasses pirater, c'est plus dans les grandes entreprises que cela se fait… »*

*D17 : « On se renseigne auprès des clients, des fournisseurs, des amis aussi. On va voir **une société de services et on se décide pour quelque chose** »*

5.4.3. Évaluation de la solution

Ensuite, l'évaluation de la réponse au besoin est réalisée de façon abstraire par les dirigeants qui mettent ainsi la SSI en perspective du besoin perçu et des renseignements obtenus, considérant notamment repose sur des caractéristiques telles que la complexité, la compatibilité et l'essayabilité. Notons que les dirigeants ont majoritairement adopté des mesures de sécurité et se prononcent davantage sur la réponse pratique mise en œuvre que sur l'évaluation mentale de la solution retenue. En effet, dans ces verbatims se conjuguent l'évaluation de la solution et l'adoption symbolique elle-même, attendu que ces dirigeants évoquent la mise en œuvre opérationnelle

Ainsi, D1 décrit son « plan de secours » en cas de perte de ses données : *« … pour moi, c'est une question de probabilités et de statistiques.* ***Il y a plusieurs couvre-feux****, mon ordinateur que* ***j'essaye d'entretenir*** *dans le sens où* ***j'ai pour habitude*** *tous les deux ou trois ans de changer d'ordinateur et de tomber en panne avec un backup sur un premier disque dur de manière à vraiment disposer d'un miroir pour disposer d'une procédure qui me permet en quelques heures d'aller racheter un ordinateur et retrouver exactement la même configuration, le backup est fait en réalité sur deux disques dur limitant alors la perte de données du premier s'il venait à dysfonctionner, lorsque je m'absente plusieurs jours, j'essaye de ne pas les stocker au même endroit pour éviter une problématique de vol ou d'incendie ou de dégât des eaux, je ne sais pas, et puis il y a encore un plan C ou le contenu des données importantes tient dans un volume assez réduit permettant de les synchroniser sur des offres cloud … ».*

D3, D5 et D6 pensent que le risque est couvert mais réfléchissent à l'amélioration de la solution retenue :

- *« Alors, est-****ce que ça couvre le risque*** *que j'avais imaginé avant le ransomware :* ***oui****. Depuis le ransomware, disons que je suis beaucoup plus sensible sur le temps de sauvegarde en fait, pas le temps mais la fréquence. Perdre une demi-journée de boulot, ça me fait ch… Donc voilà, mais par contre aujourd'hui on en est rendus à ça : c'est-à-dire qu'il y a une* ***sauvegarde qui se fait le matin et une qui se fait le*** *soir. Donc si on perd quelque chose, on perd une demi-journée de travail ».*
- *D3 : « Je pense que oui. Est-ce que c'est ce qu'il y a de plus efficace ? Je n'en suis pas convaincu. Pourquoi ? Parce qu'on a eu une deuxième attaque virale. Donc là on n'a perdu qu'une demi-journée de travail, même parce que je crois qu'on a eu de la chance car l'attaque a eu lieu juste après la sauvegarde…****Peut-être que la meilleure solution c'est d'avoir un système sauvegarde qui s'update, je ne sais***

***pas si ça existe mais, à la minute quoi, dès qu'on modifie un fichier paf ça se fait**. »*

- *D3 : « **Oui, je pense*** (que mes risques sont couverts)*. Je ne vois pas. On pourrait toujours faire plus comme je l'ai dit, oui la sauvegarde à la seconde… Jusqu'au prochain piratage où on va perdre peut-être une demi-journée et où je dirai que ça commence vraiment à me gonfler. **Pour l'instant je pense que c'est bien. »***
- *D5 : « On n'**est pas encore protégés jusqu'au bout**, il manque encore un chainon,… la sauvegarde automatique fonctionne bien sur nos PC mais il faudrait avoir une **sauvegarde de sauvegarde qui soit hébergée** … J'attends désespéramment que mon hébergeur informatique fasse un choix technique parce que j'ai une problématique de débit insuffisant »*
- D6 : (au sujet des clubs dans lesquels l'information SSI est présentée) *« ils montrent **les intérêts du cloud** et moi-même j'y **suis assez réfractaire** mais avec une connexion Internet qui permet un bon débit je vais m'y intéresser… […] Jusqu'alors on n'avait pas la fibre donc maintenant qu'on **l'a il faut que je réfléchisse à un système de sauvegarde sur le cloud directement mais je ne l'ai pas encore fait…** »*

D4 après avoir évoqué ses besoins de sauvegarde et l'influence de la réglementation sur les pratiques, émet une réserve sur la déclinaison opérationnelle des mesures de sécurité précisant qu'il s'agit, pour un dirigeant, de *« second dossier »* :

- *« … sécurisation de nos systèmes d'information internes c'est-à-dire comment on stocke nos données. On a deux types de données qui nous sont chers : c'est toute la base de connaissances que l'on produit : nos photos, nos thèmes, nos documents, tout ce qui peut émaner de chez nous donc. Pour ça **on a aujourd'hui un système informatique avec des back-up assez fréquents où j'ai conscience qu'on pourrait faire mieux […]** Après on évoquait tout ce qui est facturation, devis. Là encore, je pense que dès que la législation entre en jeu, c'est **là où on est les plus sécurisés** parce que finalement on nous impose de telles lois que la sécurisation -et là notamment je parle des factures etc… on ne doit pas pouvoir modifier une facture, chacune doit avoir un numéro unique, qui se suit, etc….*
- *« Je pense que comme tout le monde **on a notion et conscience que la sécurité est fondamentale, pas fondamentale, importante**. Si c'était fondamental ce serait*

> *quelque chose qu'**on traiterait en premier et ce n'est pas ce qu'on fait**. En fait, on se concentre sur le cœur de nos business, après on se dit qu'il faut absolument qu'on s'en occupe. Cela fait partie **des seconds dossiers qui passent après toutes les urgences et quand on y confrontés, c'est un peu le principe** de l'assurance, quand on doit payer on se dit ah mince je n'étais pas bien protégé, ah mais vous n'étiez pas assuré non plus. »*

Après avoir évoqué son constat sur la faiblesse des sauvegardes des entreprises, D4 répond : *« Je pense que **c'est de la méconnaissance**. Si demain on arrive à leur dire écoutez, ne vous inquiétez pas, vous payez… et vos postes sont sauvegardés de façon sécurisée sur le Cloud etc… ça leur va bien. ».*

D7 s'interroge sur le manque de compétence sur la mise en œuvre et le contrôle des mesures :

- *« … mais je suis convaincue que la fiabilité à 100% **n'y est pas dans ma structure**, mais comme dans quelle autre structure, **parce qu'on n'a pas suffisamment de compétences** »*
- *« Je **pressens forcément un manque de fiabilité**. Je prends ma voiture : elle fonctionne, elle fonctionne, elle fonctionne, jusqu'au jour où j'aimerais qu'on s'arrête, qu'on ouvre le capot et qu'on me dise ça c'est bon, il ne manque pas d'huile, il ne manque pas ça. Il y a ce qu'on a écrit et il y a la capacité à vérifier ce qui a été écrit. Et moi **je n'ai pas de compétences en informatique**. »*

Si D8 peut disposer des informations de son prestataire permettant d'évaluer la solution, il souligne le manque de réalisation pratique : *« …il **y a des choses dont j'ai entendu parler et qui ont l'avantage de me mettre la conscience dessus**. Après, qu'est-ce qu'on en fait réellement, je ne suis pas sûr de mettre en place grand-chose en toute honnêteté. J'y pense mais malheureusement après, pris dans le quotidien, je ne suis pas en train de réfléchir moi-même au papier que je suis en train de mettre dans ma poubelle.*

Pour D11 la solution retenue était déjà utilisée dans son poste précédent *« Donc l'idée c'est vraiment de pouvoir, du fait que ce soit dans nos propres baies sur des serveurs dédiés au sein d'un DC, quels que soient les services qu'on peut proposer à nos clients c'est toujours avoir la **maîtrise de ce qu'on peut soit utiliser soit proposer** tant sur le logiciel que sur la partie donnée »*

D16 évoque les apports de la SSI : *« Plus de vigilance, plus d'intelligence sur la gestion des données aussi. En fait, la sécurité nous permet de moins* ***disperser nos infos*** *aussi et donc de mieux les utiliser. Au début, la SSI c'était surtout pour les virus et le vol d'information. Aujourd'hui on fait* ***aussi attention à la diffusion, à la dégradation volontaire et involontaire*** *»*

5.4.4. Synthèse du processus d'adoption symbolique

La perception des besoins repose, selon les verbatims, sur la nécessité de répondre à une perte de disponibilité ou de confidentialité, vécue ou imaginée ou d'adresser directement la SSI. Par exemple, les pertes évoquées pour les risques vécus, sont la conséquence d'un ransomware, d'un piratage du réseau par le Wi-Fi, l'utilisation d'accès au SI par un informaticien dont l'entreprise s'était séparé ou encore la fraude à la carte bancaire. Pour les risques imaginés, les propos relèvent davantage de **la crainte d'une perte**, là aussi de disponibilité ou de confidentialité, à l'exception des commentaires de deux dirigeants. Ainsi D10 craint l'exposition de son SI due à ses interconnexions *« qui allaient monter crescendo »* et ainsi accroitre le nombre et la variété des failles systèmes diverses et variées. D14, quant à lui, évoque l'incendie pour caractériser sa crainte de perdre des informations.

Concernant le besoin des dirigeants pour la SSI, leurs connaissances propres, les connaissances partagées avec les membres de leur réseau d'influence ou la nécessité de se conformer à la réglementation regroupent l'ensemble des verbatims. Ainsi est évoqué la sensibilité « *au niveau personnel »* à *« ces problèmes de sécurité »* en perspective des entreprises qui sont *« sont moins bien sécurisées que nos propres données personnelles »* ou **une manière d'aborder** la sécurité selon *« le management de la qualité »* et la *« manière de manager la donnée dans (mon)* le *cabinet ».* Les besoins perçus sont également évoqués en l'absence de connaissance sur l'utilité d'un produit de sécurité (D6) pour faire comme « tout le monde ». Le besoin peut aussi provenir de la communication des institutions réglementaires telles la CNIL (D1) ou une autorité de régulation (D5) soulignant l'obligation de *« tout sauvegarder* ». Particulièrement les activités métier de D9 lui suggèrent d'assurer la confidentialité (« *c'est le secret professionnel »*) et la disponibilité (« *protection face à une mise en responsabilité* »). Il précise que cette réflexion s'est faite *« par un long cheminement » avec « des rencontres, des discussions, des expériences malheureuses de confrères ou de clients. »*

Les renseignements recherchés sur la solution proviennent, selon les verbatims, soit des expériences passées dans des postes précédents, soit des échanges avec des réseaux d'influence proche ou encore des échanges avec les organismes de formation.

Ainsi D1 évoque être un « *passionné **de nouvelles technologies » et** D14 s'informe par ses lectures des nouveautés de toute nature tel « un garçon **qui lit pas mal** ».* D2, D5 et D11 soulignent le poste qu'ils ont occupés précédemment réciproquement dans l'industrie militaire *« un cadre assez sécurisé »,* dans une fonction où il s'agissant « *au quotidien **de mettre en garde** »* sur des problématiques de préservation des données et enfin dans l'informatique comme origine de leurs connaissances et de leurs pratiques. D9 a des habitudes liés à son service militaire dans les transmissions et précise qu'il est *« … habilité »* et *« **sensibilisé à ces questions**-là… ».* D2 et D11 évoquent **des formations** dans lesquelles un consultant de la DST leur transmettait des « »bonnes pratiques » en termes de SSI.

Les renseignements sur la solution sont aussi issus d'amis ou de prestataires. D3 souligne les échanges avec un « *copain qui a 3 ou 4 sociétés »* et qui lui fait valoir la maitrise de sa SSI, D9 évoque des échanges avec *un « ami spécialiste en sécurité ».* Les échanges avec des clubs ou des associations sont cités pour s'informer sur les solutions (D8 et D14). D13 et D16 précisent indique qu'il s'appuie sur *« l'expérience des particuliers et des professionnels »* de son entourage pour s'informer et *« chaque fois que je vois quelqu'un qui a eu un problème, j'essaie d'en tenir compte et de voir comment je peux faire dans ma boîte pour éviter la même chose… ».* Les prestataires, bien que définis comme membre de réseau d'influence semblent avoir un rôle particulier pour plusieurs dirigeants (D3, D6, D8 et D13).

Les verbatims mettent en évidence les avantages de la solution retenue pour répondre au besoin. Ainsi les mesures de sauvegarde multiples et complémentaires mises en œuvre sont évoquées (D1, D5, D6 et D7) pour indiquer que la SSI est une « bonne solution ». On note cependant que ces solutions pourraient être améliorées (D3, D5 et D6). D4 et D8 rapportent que s'ils sont conscients de la SSI comme solution aux risques qu'ils considèrent, ils émettent des réserves sur l'opérationnalisation de sa déclinaison.

Perception des besoins	*« Par rapport à mon expérience, … mais oui victime à l'époque des CD beaucoup… j'ai perdu des photos qui étaient sur le CD »* *« …bon on a quand même pris un **ransomware !** … pour ne pas être embêtés ou du moins le moins possible en cas de rebelote sur des ransomware ou des choses comme ça »* *« … ça nous a fait prendre conscience **qu'il fallait peut-être sauvegarder** les données parce qu'on s'est dit que si on venait à perdre des jours des jours des jours comme ça … ce serait des milliers d'heures de perdues »* *« …depuis un véhicule des gars avaient **piraté le Wi-Fi** et étaient rentrés dans notre SI administratif … et en fait, avaient récupéré des données qui était dans ce SI »* *« Ce qui me pousse à sécuriser … ce qui m'a toujours inquiété c'est qu'est-ce qu'on fait si on n'a plus de poste informatique ? D'abord **la perte de données** pure et dure … la perte d'informations qui peut mettre tout le monde au chômage »* *« Mon père effectivement étant policier m'a toujours transmis de toujours faire attention… j'ai un tempérament **un petit peu suspicieux »*** *« … personnellement, j'agis par le management de la qualité …. C'est ma manière de manager la donnée dans mon cabinet »* *« En fait lorsqu'on devient courtier, on est **obligés de tout sauvegarder** parce que les compagnies n'ont plus le même fonctionnement qu'avec ses agents. »* *« Le premier c'est le **secret professionnel** qui fait qu'effectivement on doit avoir une notion de l'information qu'on protège, qu'on sécurise, qu'on ne divulgue pas, etc… Le deuxième c'est **la protection face à une mise en responsabilité**, c'est-à-dire c'est le **fait de conserver des données** … »*
Renseignement sur la solution	*« … le coté informatique m'intéresse à titre personnel donc je **ne suis pas démuni lorsqu'on me dit il faut sauvegarder je sais ce que ça veut dire**, je sais comment le faire je sais où le faire. »*

	« Quand on travaille dans ce qui s'appelle maintenant « industrie d'hélicoptères militaire », on est ***forcément confronté à un cadre assez sécurisé****. »* *«* ***c'était mon métier*** *! … je connaissais ça au quotidien* ***de mettre en garde*** *aussi sur le plan juridique sur le plan fiscal,* ***sur le plan des données****… »* *«* ***De moi*** *!* ***Je n'ai pas de connaissances mais je suis à l'ancienne*** *alors que le cloud n'existait pas il y a 10 ans, je vous le rappelle, et donc j'ai grandi avec des disques durs et des disquettes molles et* ***j'ai gardé mes habitudes de mes disques durs auprès de moi pour faire des sauvegardes….*** *[…]* *« …j'ai effectué* ***mon service militaire je le fais dans la transmission****… donc je suis habilité et on est* ***sensibilisés à ces questions****-là… »* *« …* ***j'étais dans la partie informatique*** *enfin quand on fait la physique on fait beaucoup de théorie et de modélisation tout passe par des gros calculateurs les fameux "****grid" »*** *« …* ***qui lit pas mal****, donc lire, parler avec des gens, voir comment ils fonctionnent et peut-être aussi à l'armée où j'ai* ***appris des façons de de faire. »***
Évaluation de la solution	*« Alors, est-ce que ça couvre le risque que j'avais imaginé avant le ransomware : oui… »* avec *« sauvegarde qui se fait le matin et une qui se fait le soir. «* *«* ***On n'est pas encore protégés jusqu'au bout****, il manque encore un chainon,… la sauvegarde automatique fonctionne bien sur nos PC mais il faudrait avoir une sauvegarde de sauvegarde qui soit hébergée »* *« .. du fait que ce soit dans nos propres baies sur des serveurs dédiés au sein d'un DC, quels que soient les services qu'on peut proposer à nos clients c'est toujours avoir la* ***maîtrise*** *de ce qu'on peut soit utiliser soit proposer tant sur le logiciel que sur la partie donnée »* *«* ***Il y a plusieurs couvre- feux****, mon ordinateur que j'essaye d'entretenir dans le sens où j'ai pour habitude tous les deux ou trois ans de*

	changer d'ordinateur et de tomber en panne avec un backup sur un premier disque dur de manière à vraiment disposer d'un miroir pour disposer d'une procédure qui me permet en quelques heures d'aller racheter un ordinateur et retrouver exactement la même configuration *« ..il y a des choses dont j'ai entendu parler et qui ont l'avantage de me mettre la conscience dessus. Après, qu'est-ce qu'on en fait réellement, je* ***ne suis pas sûr de mettre en place grand-chose en toute honnêteté*** *»*

Tableau 17 : Synthèse des éléments du processus d'adoption symbolique

5.5. Réponse pratique au risque, mise en œuvre de la SSI

Les verbatims montrent quelques contraintes du passage de l'adoption symbolique à la mise en œuvre pratiques, ou plus généralement, les solutions adoptées.

5.5.1. Absence de mise en œuvre

D12 évoque des difficultés d'organisation afin d disposer de mesures de sécurité quant aux accès au SI : *« …mon CTO est parti en vacances il* ***a fallu réinitialiser les box pour*** *retrouver les accès, c'était un petit peu compliqué peut-être un petit peu trop d'ailleurs »*

Des contraintes financières sont avancées par D3 D4, D6 et D16 comme freins à l'adoption :

- *D3 : (à propos d'un service plus efficace de sauvegarde) « Si, je pense qu'ils le proposent mais* ***il y a un coût qui est plus important*** *que ce que j'ai mis en place. »*
- *D3 : « C'est comme pour l'alarme si vous voulez. L'alarme -bon on a déménagé cette année, avant on était dans l'autre partie du bâtiment- et donc on avait une société et ils sont venus nous* ***dire que notre système était obsolète, qu'il fallait renforcer****. J'ai dit vous savez ce qu'on va faire, on va* ***arrêter la télégestion*** *parce que finalement vous nous servez à rien ! Quand il y a un truc c'est qu'il y a un courant d'air, on a mal fermé une fenêtre.* ***Si je fais déplacer quelqu'un ça coûte 300€*** *et vous me réveillez en pleine nuit pour rien. Et j'ai arrêté la télégestion. »*
- *D4 : « Aujourd'hui, on a étudié les possibilités justement de serveur-miroir, ce genre de choses, et pour l'instant* ***c'est hors de notre budget****. » et « … je me dis voilà, en moyenne on va avoir 1 ou 2 jours de down dans l'année, ça me coûte combien, combien ça me coûte de mettre en place ? Pour l'instant, je préfère encore perdre 1 ou 2 jours de CA mais le jour où je vais me dire que le jour de CA il est remboursé et me paie 5 ans de serveur-miroir, la* ***décision ne sera pas difficile à prendre et*** *on* ***basculera sur la sécurisation****. »*
- *D6 : « …* ***si j'avais plein d'argent je pourrais*** *me mettre au niveau de Microsoft ou la NASA mais* ***n'aillant pas de sous*** *je me contente de ce que j'ai, chaque mesure mise en place c'est un truc en plus qu'on se rajoute : on part de très loin quand on voit d'où on vient avec Avast et des ordinateurs locaux avec des Windows même pas pro et petit à petit on découvre les besoin et* ***on les finance*** *»*

- *D16 : « Enfin, c'est le projet parce qu'après il faut avoir **le temps et l'argent** pour mettre des choses en place : il faut bien gérer les urgences et le business est prioritaire. »*

5.5.2. Mise en œuvre

Dans le prolongement des propos révélant l'adoption de la SSI, nous mettons en perspective la mise en œuvre pratique relevée par les interviewés et concernant la sauvegarde de données, les logiciels pour contrer les virus ou encore les pare-feux :

- *D1 : « Alors après ça dépend des métiers, en photo il faut gérer un volume de donnée en terme de taille qui est colossal… Moi depuis. 2009 j'ai notamment une partie de mes outils **de travail qui sont synchronisés sur un une DropBox** »*
- *D1 : « donc c'est plus facile à manier je peux acheter deux clés pour avoir deux sauvegardes, ce n'est pas quelque chose de très coûteux et très compliqué et puis après avoir un logiciel qui synchronise les données suffit »*
- *D1 : « sur MAC **cette sauvegarde TimeCapsule** qui est un programme natif de synchronisation et qui va au-delà de synchroniser les données, l'avantage c'est que si mon ordi tombe demain, j'en rachète un autre et je le replug en quelques heures je retrouve jusqu'aux icones sur mon bureau tout exactement pareil. Donc effectivement c'est une sécurité, cette sauvegarde je **la fais deux fois sur deux supports différents on commence à limiter un petit peu les risques** ».*
- *D2 : « Régulièrement, il faut que je le fasse, je fais une sauvegarde sur un disque dur externe, c'est assez sommaire comme mesure, gravement ! »*
- *D3 : « En plus aujourd'hui on a mis en place les NAS qui copient et dupliquent chez moi donc je suis un peu plus tranquille on va dire … »*
- *D6 :* (s'agissant de l'antivirus) *« Oui parce que **c'était gratuit, je ne savais pas à quoi cela servait**, … alors je prenais des versions gratuites, jusqu'à maintenant j'ai la chance… »*
- *D6 : « Oui **je faisais de la sauvegarde des fichiers stratégiques sur cloud ou des sauvegardes sur disques externes**… »*
- *D8 :« …aujourd'hui j'ai un disque externe avec un double disque, un qui est chez moi et un ici que je fais tourner une fois par semaine avec une duplication des données tous les jours. Ça duplique et ce n'est pas juste de l'incrémentiel ».*

- *D9 : « C'est les pare-feux, les anti-intrusions du système informatique qui **j'espère nous protègent efficacement** d'une cyber-attaque. »*
- *D17 : « …on **a des logiciels de sauvegarde** quand même plus perfectionnés que Drive ou Dropbox. Certaines choses sont synchronisées en auto. […] ..dans les bureaux, on a des **armoires sécurisées avec des codes**. Nos ordinateurs sont protégés. On peut toujours se faire voler mais on a commencé à mettre des obstacles même si je ne pense pas que ça marche à 100%. […] par exemple, nous n'avons pas de broyeur ! C'est peut-être un problème »*

D'autres pratiques pour contrer des menaces de nature différentes sont également évoquées :

- *D2 : « Sur la sécurité, on est forcément **préoccupé par ne pas laisser son sac**. Quand je pars de chez moi, je ne laisse pas l'ordinateur dans la sacoche si je ne l'emporte pas avec moi. **Je le mets dans un autre endroit**. »*
- *D2 : « Quand **je planque mon ordinateur**, là c'est clairement contre le cambriolage, le vol à la maison. Ici, en termes de **protection, c'est le stock**. À l'atelier, on a quand même du matériel, il n'y a pas d'alarme. Il faut le savoir, il faut avoir envie de venir, mais par définition on pourrait très **bien se faire piquer du matériel, des appareils photos, des choses comme ça.** »* et *« Si je m'arrête en ville pour boire un verre ou autre par ex. **je ne laisse jamais mon PC dans la voiture**. Je le prends sur mon dos.* »
- *D2 : « Et malgré **ça un destructeur de papier, oui**. Un destructeur, ça coûte 40€, je le prends en me disant que ça servira toujours et quand j'imprime une facture de travers, je la passe au destructeur. **C'est plus un réflexe, pour faire bien en fait**, pour me dire j'ai fait quelque chose de bien. Mon client ne le voit pas **mais je respecte ce document qui lui est destiné** et qu'il n'y a pas pour moi à prendre un seul risque qu'il se retrouve dans une poubelle éventrée à la déchetterie, à traîner. »*
- D8 : « On a **un broyeur mais je dois être le seul à l'utiliser** sur des documents un peu sensibles parce qu'à mon avis tout le monde s'en f… un peu. »
- *D13 : « Après maintenant de toute façon la **sécurité est un paquage**, on se protège pas que pour le **piratage** on se protège pour tout on se protège des **accès** pour que personne puisse rentrer on le fait pour ne pas **perdre** de données… »*
- *D14 : « Je fais des **sauvegardes** de toute façon. Si ça m'arrive, j'ai ma clé USB de sauvegarde et **je remets tout sur un autre poste**. »*

D4, quant à lui, souligne des pratiques en réponse à des exigences réglementaires : *« toujours chez le client, c'est la sécurisation des données. Depuis le début nous, là on s'y attelle. … **on demande à chacun des clients qui s'inscrivent sur notre compte s'ils veulent recevoir la newsletter**. Donc vraiment le côté opt in/opt out, c'est quelque chose **qu'on respecte énormément**. Peu le font, je le sais, je le remarque tous les jours mais ce n'est pas grave, nous on le fait et donc si vous voulez, **avec la législation qui est passée en mai sur le côté RGPD** c'est quelque chose qui rentrera dans les principes ».*

En complément D10 et D11 énoncent respectivement des mesures visant à s'appuyer sur les services d'experts et des procédures, D12 assoit ses mesures sur son hébergeur :

- D10 : (après un piratage important) *« à l'époque la sécurité des systèmes s'est renforcée et on a mis en place des pare-feux et des antivirus et aujourd'hui on se fait accompagner d'experts sur ces problématiques »*
- D11 : *« D'où effectivement dans l'usage du CRM on a **mis quelques procédures pour pouvoir empêcher ce genre de choses** ».*
- D12 : *« Mon hébergeur est **un grand spécialiste** de la sécurité en France. On lui a expliqué ce qu'on faisait et que notamment les données après quelques jours sont copiées sur un serveur d'archivage et qu'on a plus besoin d'un accès rapide, dans ce cas-là je prends un serveur moins puissant mais avec des gros **des disques durs en RAID6**, c'était sa réponse à la problématique… »*

5.5.3. Compétences mobilisées

Les verbatims montrent une majorité d'interventions de compétences externes à l'entreprise pour la mise en œuvre des mesures. Précisément, les prestataires ont un rôle omniprésent dans l'approche de la SSI par les dirigeants. Ainsi il apparait que si leur influence peut parfois être associée à un conseil « à suivre », majoritairement elle semble critiquée.

Ainsi, D3 et D5 évoquent le conseil de leur prestataire sur des risques potentiels pour leur SI :

- *D3 : « Et là c'est ma **faute parce que le prestataire informatique m'avait dit** quand même il faudrait que tu déportes ta sauvegarde, c'est important. Et moi je disais de toute façon si on brûle, la sauvegarde sera dans le bâtiment alors ! **Il m'a dit "tu fais comme tu veux, moi je t'ai prévenu !" »***

- *D5 : « Au fil des discussions avec mon prestataire et mon cabinet comptable, … on a les mêmes problématiques en fait et je crois qu'il y a* ***une transmission d'angoisse****… aussi on s'aperçoit que* ***quelle que soit la profession, en tout cas dans ces professions là, ce serait vraiment dramatique*** *effectivement* ***de perdre des données*** *»*

D'autres verbatims, montrent, à l'opposé, que les prestataires ont des pratiques inadaptés sur lesquels les dirigeants s'interrogent :

- *D3 : « … il y a un an on a pris un virus ransomware et là on s'est dit ''oh, alors là c'est la m…, vraiment !'' […] pour sécuriser notre système informatique mais pas tant en termes de mots de passe et de choses comme ça parce* ***que la société informatique que j'emploie nous avait dit qu'on a un Cisco et que c'est vachement bien****… bon on a quand même pris un ransomware »*
- *D7 : « …* ***Parce que je pense que mon interlocuteur raconte des c… »***

Précisément, D8 narre un incident pour lequel son prestataire n'a pas été en mesure de restaurer ses données, en faisant valoir que le poste de l'entreprise était vieillissant : « *''ah oui oui, mais en fait* ***il n'y a pas de sauvegarde****''. ''Comment ça il n'y a pas de sauvegarde ? Normalement il y a une sauvegarde tous les soirs, elle est chez vous, elle est censée être faite. Moi je n'ai pas eu de perte de connexion réseau, où sont les sauvegardes ? '' C'est l'excuse qu'ils m'ont donnée, je n'ai pas vérifié mais j'apprends qu'en fait les sauvegardes elles sont bien faites et que potentiellement, le problème venait justement -comme par hasard- de mon PC qui commençait à avoir des signes de fatigue, qui envoyait en fait des sauvegardes vérolées sur leur serveur.* ***Ils m'ont enfumé****, je le sais, ils le savent car je leur ai dit* ***qu'ils me prenaient pour un c…*** *Parce qu'en fait, en gros, ils sont en train de me dire que leur logiciel, génère une sauvegarde sur mon PC et que mon PC la transmet.* ***Ce n'est pas ça qui se passe, je le sais****. En fait il y a une synchronisation des données en permanence chez eux et donc il n'y a pas de fichier qui se crée puisque quand je leur demande de me dire quel est le fichier qui se crée et qu'ils reçoivent ils sont incapables de me dire de quoi il s'agit. S'il y a un fichier qui se crée sur mon poste, je voudrais savoir physiquement où est-ce qu'il se crée. Et donc ils me disent ça fait 3 mois que c'est vérolé*

5.6. Commentaires des interviewés lors des entretiens

Plusieurs interviewés ont partagé leurs réflexions lors de l'entretien, soit à propos de leurs pratiques en regard de l'état de l'art qu'ils imaginent ou connaissent, de leur besoin, ou encore de commentaires directement en lien avec le fait d'évoquer la SSI :

- *D2 : « Au départ j'ai une sauvegarde ça me suffit.* ***Aujourd'hui, grâce à vos questions****, ça me fait refaire* ***le tour de notre dispositif****. Je ne savais vraiment pas vers quoi on allait aller avec cet entretien. Et du coup, grâce à ce questionnement, je me dis que* ***finalement ce n'est pas si mal pour la sécurité à minima*** *liée à l'activité, en gros, la perte d'activité. On maîtrise au minimum nos données, c'est le sentiment que ça me donne.* ***Par contre, peut mieux faire*** *et si on veut gagner en performance/productivité, là j'ai le sentiment qu'il faut aller un petit peu plus loin, notamment sur le fait que si on me pique l'ordinateur, ça date, ça fait peut-être 1mois et demi que je n'ai pas fait ma sauvegarde »*
- *D3 : « Oui, au fil de notre discussion, l****a prise de conscience qu'il y a peut-être moyen d'améliorer notre système et que je n'ai peut-être pas forcément pris la bonne option.*** *Mais bon, j'ai mis ça en place et pour l'instant je ne vais pas forcément consacrer un budget plus important là-dessus. Je pense que le rapport prix-sécurité de ce qu'on a mis en place me paraît bon. »*
- *D4 : « On prie pour que ça aille vite, c'est tout ce qu'on a à faire ! Aujourd'hui, on a étudié les possibilités justement de serveur-miroir, ce genre de choses, et pour l'instant c'est hors de notre budget. Là encore, c'est ce que je disais tout à l'heure, on essaie d'orienter notre budget un peu et* ***rien que le fait d'en parler, il y a longtemps que je n'y avais pas pensé****, il faut que je m'arrête sur cette question : il faut qu'on ait une solution parce qu'aujourd'hui on a 2 jours -je crois que le pire qu'il nous ait fait, sans accès au site Web plus de 24 heures qui était down ! ».*
- *D4 : « Ça fait partie de la stratégie marketing d'intégrer* ***cela et plus je vous parle et plus je suis en train de me dire qu'on a des tas de choses à faire.*** *»*
- *D6 : (évoquant les raisons pour lesquelles ses collaborateurs ne sauvegardent pas) « Parce qu'ils n'ont jamais rencontré de grosses merdes avant... Ils ne se rendent pas compte de l'impact que cela peut avoir… oui je pense que quand ça vous est arrivé, ça vous marque… »*
- *D17 : « Mais* ***maintenant que j'y pense****, j'ai peur pour le vol de données surtout celles qui sont dans des rapports un peu confidentiel et que l'on a en interne mais que l'on a fait pour ces clients. Va falloir que* ***l'on y réfléchisse plus car c'est peut-***

être de plus en plus important ces choses-là*. »* et *« **Avec vos questions**, je me demande si on **ne doit pas aller plus loin** que ce que nous avons mis en place sur la protection des données surtout. […] Ça sera peut-être plus cher mais pour certainement plus efficace. **Ça peut aussi jouer sur l'image de marque et donc nous amener plus de clients »***

5.7. Synthèse des résultats de la recherche

Afin de synthétiser nos résultats, nous dressons un synoptique de l'adoption de la SSI, par la connaissance des risques, l'approche retenus et les contraintes évoquée pour la mise en œuvre

	AS de la SSI	**Contraintes à l'AS**	**Connaissance du risque**	**Approche de la réponse au risque**	**Connaissances des solutions**
D1	Oui	Non	- Proches (perte des photos du père) - Dysfonctionnement dans son entreprise précédente - Dysfonctionnement sur son SI (mineur) Risque vécu : oui Risque connu : oui	- Préventive pour la perte de service / données - Réactive pour la réglementation Centrée sur le fonctionnement de ses process majeurs	- Passionné d'informatique - Reproduction des pratiques : o Du père (disponibilité) o De l'entreprise précédente (confidentialité)
D2	Oui	Non	- Proches (pratique proactives basée sur l'expérience d'autres) - Dysfonctionnement dans son entreprise précédente (étudiant) Risque vécu : oui Risque connu : oui	- Préventive pour la perte de service / données Centrée sur le fonctionnement de ses process majeurs et l'image pour ses clients	- Grace à un associé - Reproduction des pratiques de l'entreprise précédente (confidentialité)
D3	Oui	Non	- Dysfonctionnement sur son SI (majeur) Risque vécu : oui Risque connu : **non**	- Réactive pour la SSI Centrée sur la conservation de ses données	- Ne s'y intéresse pas particulièrement - Repose sur son prestataire

	AS de la SSI	**Contraintes à l'AS**	**Connaissance du risque**	**Approche de la réponse au risque**	**Connaissances des solutions**
D4	Oui	Non	- Perte de ses données professionnelle dans l'activité antérieure à son entreprise Risque vécu : oui Risque connu : oui	- Préventive pour la perte de service / données - Préventive pour le respect des lois Centrée sur le fonctionnement avec ses clients (vente, service après-vente)	- Par son expérience professionnelle passée
D5	Oui	**Oui**, imposée par la réglementation	- Perte de ses données professionnelle dans l'activité antérieure à son entreprise Risque vécu : oui Risque connu : oui	- Réactive pour la perte de service / données - Réactive pour le respect des lois Centrée sur le temps de restauration (manuel, perte de données)	- Par son expérience professionnelle passée - Par ses échanges avec son réseau professionnel et prestataire
D6	Oui	Non	- Expériences professionnelles antérieures - Échanges avec « des clubs » Risque vécu : oui Risque connu : oui	- Réactive pour la perte de service / données Centrée sur la conservation de ses données	- Par son expérience professionnelle passée - Par ses échanges avec les clubs et les prestataires
D7	Oui	Non	- Expériences professionnelles antérieures - Échange de pratiques avec un professionnel de son métier (confidentialité / secret professionnel) Risque vécu : oui Risque connu : /	- Réactive pour la perte de service / données Centrée sur la conservation de ses données	- Peu d'intérêt pour la solution, active la « délégation »
D8	Oui	Non	- Expériences professionnelles antérieures Risque vécu : oui	- Préventive pour la perte de service / données Centrée sur la conservation de ses	- Intérêt manifeste pour les solutions techniques - Par ses échanges avec les clubs et les prestataires

	AS de la SSI	Contraintes à l'AS	Connaissance du risque	Approche de la réponse au risque	Connaissances des solutions
			Risque connu : oui	données	- Par ses échanges avec « un ami spécialité »
D9	Oui	Non	- Expériences professionnelles antérieures - Échange de pratiques avec un professionnel de son métier (confidentialité / secret professionnel) - Échange avec un « ami spécialiste » Risque vécu : oui Risque connu : oui	- Préventive pour la perte de service / données Centrée sur la conservation de ses données	- Par des échanges avec un « ami spécialiste » - Par ses échanges avec les prestataires spécialisés
D10	Oui	**Oui**, imposée par la réglementation	- Expériences professionnelles antérieures - « Suspicieux » Risque vécu : oui Risque connu : oui	- Préventive pour la perte de service / données - Préventive pour le respect des lois	- Par ses échanges avec les prestataires spécialisés
D11	Oui, « security by design »	Non	- Par l'expérience, par la veille pour son activité (SI) Risque vécu : oui Risque connu : oui	- Préventive (n'attend pas de vivre l'incident pour mettre en œuvre)	- Par sa formation, son poste précédent
D12	**Non**	Non	- Par l'expérience Risque vécu : oui Risque connu : oui	- Pas de réponse au risque (remet à plus tard les réponses)	- Par ses échanges avec les prestataires spécialisés
D13	Oui	Non	- Proches (personnel et professionnel / pratiques	- Préventive (apprentissage par les retours d'expérience des autres)	- Par ses échanges avec son prestataire informatique

	AS de la SSI	Contraintes à l'AS	Connaissance du risque	Approche de la réponse au risque	Connaissances des solutions
			proactives basée sur l'expérience d'autres) Risque vécu : non Risque connu : oui		- Par ses échanges avec des proches
D14	Oui	Non	- Par l'expérience Risque vécu : non Risque connu : oui	- Préventive (adoption de support papier)	- Par son réseau d'influence - Par ses lectures
D15	Oui	Oui	- Par l'expérience Risque vécu : oui Risque connu : non	- Pas de réponse au risque (pense qu'il n'y est pas exposé)	- Par son hébergeur
D16	Oui	Non	- Par l'expérience acquise dans son ancien poste - Risque vécu par des partenaires / prestataires Risque vécu : oui Risque connu : oui	- Préventive pour la perte de service / données Centrée sur la : - confidentialité en regard de sa R&D et de l'impact d'une divulgation de données - disponibilité pour le service à ses clients	- Par son expérience professionnelle passée
D17	Oui	Non	- Par l'expérience Risque vécu : oui Risque connu : oui	- Préventive pour la perte de service / données	- Par son réseau d'influence - Par ses échanges avec les prestataires spécialisés

Tableau 18 : Synthèse des résultats de la recherche

Chapitre 6. Interprétations et discussions

Notre recherche ambitionne de progresser dans l'intelligibilité des éléments considérés lors de la décision d'adopter symboliquement la sécurité des systèmes d'information. Ainsi, dans le présent chapitre, nous allons confronter les cadres théoriques mobilisés, notamment la perception des risques et le management des risques SI, avec les résultats présentés tout au long de la section précédente. Le projet de cette discussion sera donc de proposer des éclairages originaux sur notre problématique de recherche, « **quels sont les éléments considérés et leur influence sur la décision d'adopter symboliquement la SSI ?** ».

Nous proposons de traiter ce questionnement général selon les perspectives théoriques de la SSI, de la perception des risques et des comportements isomorphiques, en organisant notre discussion autour des deux questions de recherche, précises et opérationnelles, qui ont été présentées dans la première partie de ce document.

La première question « **Quels sont les éléments considérés dans la décision d'adopter symboliquement la SSI? »** vise à mieux saisir les éléments considérés lors de la réflexion, qu'il s'agisse de risque, de SSI, de réglementation ou, encore, de caractéristiques propres au dirigeant et son réseau d'influence. Nous répondons à cette question en exposant l'ensemble des éléments considérés, d'une part lors de la décision et d'autre part tout au long du parcours du dirigeant, notamment avant qu'il prenne sa fonction au sein de l'entreprise. Précisément, il s'agit de présenter ces influences sur la décision de la SSI dans le prolongement des travaux de Straub et Welke (1998) ou, plus particulièrement, des travaux sur l'importance des SI (par exemple Mcfadzean et al. 2007) ou des risques pris en compte pour la SSI (par exemple Albrechtsen et Hovden 2009 ou Huang et al. 2010).

La deuxième question « **Comment ces éléments influencent la décision d'adopter symboliquement la SSI ? »** a pour objectif de mettre en perspective, dans la réflexion conduisant à la décision, les éléments considérés lors du processus d'adoption symbolique. Autrement dit, les influences sont analysées en regard des trois étapes de l'adoption symbolique. Nous aspirons à décrire comment ces influences interagissent dans la réflexion du dirigeant pour décider d'engager la SSI. Il s'agit de rendre intelligible ces influences en regard de la décision pour la gestion du risque SI.

6.1. Éléments considérés lors de la décision d'AS

Dans cette première partie, nous observons la vision du dirigeant sur le SI et les risques dans la perspective de caractériser les éléments qui sont pris en compte. Notre propos n'est pas de mesurer l'influence de ces éléments mais d'identifier lesquels émergent de notre terrain afin de les discuter à partir des théories que nous avons mobilisées. Précisément, il s'agit de décrire les éléments, tels que la perception des risques, les influences internes et externes de l'entreprise, qui peuvent alimenter la réflexion des dirigeants sur la gestion des risques et la SSI.

6.1.1. L'importance des SI au cœur du regard sur la SSI

Pour commencer, nos résultats montrent que **l'importance des SI est particulièrement soulignée par les dirigeants**. Ainsi le système d'information est considéré comme *« élément indispensable car organisationnel »*, *« très important »* et « *devenu évidemment très central ».* Si cette importance ne relève pas toujours d'un rôle « stratégique » pour le développement de l'activité, elle est décrite en regard de l'usage qui en est fait et d'un support à la conformité réglementaire. Rappelons que Bharadwaj et al. (2013) situent le SI au cœur des activités des organisations et que plusieurs auteurs précisent le lien entre **l'importance considérée du SI et l'engagement pour la SSI des dirigeants** (McFadzean et al. 2007 ; Solms et Solms 2006b ; Wood 1995). L'importance du SI est aussi soulignée comme support d'activités spécifiques contrôlées par des autorités de régulation ou d'outil de coordination des acteurs de l'entreprise rejoignant alors les commentaires de Kankanhalli et al. (2003) et de Sambamurthy et al. (2003) qui mettent en évidence le rôle du SI dans l'amélioration des capacités organisationnelles.

Une fois établie l'importance accordée au SI, nos résultats montrent aussi l'importance de la SSI, à l'appui de commentaires qui mettent en perspective l'association de l'activité « SI » et l'entreprise même, ou, encore, des risques plus techniques. Les exigences de disponibilité et de confidentialité sont abordées et leur respect est précisé en fonction du SI et de l'organisation :

- la confidentialité des projets et des informations : *« …cela a même été imposé, de garder le projet confidentiel »* et *« Éviter la diffusion d'informations, diffusion externe soit sur la concurrence, soit sur des clients en particuliers ».*
- la disponibilité du SI et de ses services : « *si l'organisation a été mise dans l'incapacité de travailler. C'est-à-dire que c'est le clash qui fait que tout s'arrête »* et *« que le service soit toujours accessible pour les centres d'appels ».*

La SSI est évoquée par la perte possible du *« fonds de commerce »* en regard d'une protection insuffisante des données : *« … pour moi c'est surtout la protection des données, la protection des données de mon propre cabinet … si je perds ça, demain, c'est assez problématique ! ».* La protection des éléments techniques du SI est également considérée dès lors que la SSI est évoquée : « *Il s'agit de **protéger** nos informations des **virus, du vol, du détournement** et, tout simplement, des ennuis dus aux **pertes ;** si on perd ou on casse un ordi, un téléphone, moi, ma secrétaire, mes collaborateurs… ».*

Les exigences de confidentialité et de disponibilité sont convergentes avec l'approche de la SSI décrite dans la littérature et particulièrement par Bishop (2003) et Whitman et Mattord (2009) qui définissent la SSI comme le **processus de protection** de la **confidentialité** et de la **disponibilité** de l'information (avec l'intégrité, que les interviewés n'ont pas mentionnée). En ce sens, nous résultats sont convergents avec les définitions centrées sur **les aspects techniques** du SI comme celle de Whitman et Mattord (2009 p. 8) pour qui la SSI est « la protection d'informations et ses éléments critiques, y compris les systèmes et le matériel ». Au sens de la protection de l'IT, Bandyopadhyay et al. (1999 p. 437) soulignent également la nécessité de « protéger des actifs informationnels comme […] le matériel ». Rejoignant cette vision technique, Gerber et Solms (2005) et Tsohou et al. (2006) mentionnent une possible approche de la SSI en considérant la perception des risques associés aux ressources informationnelles support (IT).

Plus largement, la SSI est considérée comme « ***fondamentale**… »* selon plusieurs perspectives pour le SI et pour ces actifs matériels, ou, davantage, pour l'activité elle-même et par extension l'entreprise. Ces commentaires sont en accord avec deux notions développées dans la littérature. D'une part, ils indiquent une **dépendance forte entre le SI**, les activités de l'organisation et le besoin de le protéger (Backhouse et Dhillon 1996 p. 2). D'autre part, comme le soulignent Peppard et Ward (2004), cette dépendance est telle que l'arrêt du **SI provoquerait l'arrêt de l'activité de l'organisation**. Nos résultats offrent un éclairage particulier sur la notion de **responsabilité** du SI et de la SSI portée par la direction générale. En effet, la responsabilité est soulignée par plusieurs dirigeants qui évoquent, par exemple, que *« s'il y a une difficulté, une erreur, in fine, c'est moi qui suis responsable* ». Ce résultat est cohérent avec ceux de Hu et al. (2007), Moulton et Coles (2003), Solms et Solms 2006a, 2006b ; Straub et Welke (1998). Précisément, la SSI est une « *protection face **à une mise en responsabilité**, c'est-à-dire de conserver des données qui ont permis de mettre en place des situations, mise en place que **l'on pourrait nous reprocher ensuite… ».*** La responsabilité de protéger ou non le SI de l'organisation s'inscrit ainsi dans l'objectif de

devoir gérer et supporter les conséquences de la survenance d'un risque et de devoir en référer au comité de direction et aux parties prenantes de la société. En ce sens, devoir expliquer au client les raisons d'un recueil de factures déjà émises est souligné (« *Quand vous devez appeler un client pour lui dire : pouvez-vous me renvoyer votre bon de commande parce qu'on ne sait pas où il est passé, même si vous dites on a eu un problème informatique,* ***c'est une position embêtante »).*** Un commentaire identique a été dressé lorsqu'il s'agit de recontacter le fournisseur pour des raisons similaires au constat ci-avant. Spécifiquement pour les clients, l'image même de l'entreprise et de son dirigeant sont considérées ***«*** *quand un site est ralenti c'est pénible et* ***donne une mauvaise image,*** *quand le service client ne répond pas, on a* ***une mauvaise image****… ».* Ainsi, ces commentaires s'inscrivent directement dans les notions développées par plusieurs auteurs sur la responsabilité du top management qui doit assurer le succès de l'organisation et a donc la **responsabilité de protéger ses SI** (Goodhue et Straub 1991 ; McFadzean et al. 2007 ; Solms 1996, 2000, 2006 ; Straub et Welke 1998).

Dans le prolongement de nos constats sur l'importance du SI et la SSI, nous remarquons la **proximité des champs lexicaux** entre la caractérisation des **risques perçus** par les interviewés et **la gestion des risques SI**. Ainsi, les interviewés évoquent les risques avec des termes tels qu'*inquiétude*, *malheur, drame, catastrophe, accident, péril, anéantissement, et problème*. Si ces termes mêlent la conséquence telle que « dramatique » ou « catastrophique » l'inquiétude est directement liée au sentiment et à la perception. Ainsi Kermisch (2012 p. 7) précise que la discipline de gestion du risque offre un « outil conceptuel riche » qui « rend compte du risque compris comme représentation des **inquiétudes individuelles** et collectives ». Ces inquiétudes reflètent le **manque de connaissance sur le risque SI**, ses probabilités et conséquences, en accord avec un des concepts fondamentaux du risque, l'incertitude, mettant en cause la **réalité même du risque**, dont la certitude dépendrait justement d'un résultat attendu et donc connu (Yates et Stone 1992).

Ces constats renforcent alors la thèse de ceux qui soutiennent que la SSI est **une discipline de gestion des risques** (Choobineh et Dhillon 2007 ; Hu et al. 2007 ; Kayworth et Whitten 2010 ; Straub et Welke 1998). Dans le prolongement de ce commentaire sur l'importance considéré du SI et de la SSI, nous pouvons maintenant aborder, justement dans une perspective de gestion des risques, les résultats sur la perception et la connaissance des risques, sur les menaces, sur les conséquences et sur l'exposition au risque.

6.1.2. Des risques souvent définis partiellement

L'importance accordée à la problématique de la protection du SI est traduite par l'expression des **risques potentiels** qui pourraient impacter le SI. En effet, soit les risques sont énoncés seuls, tels un « danger », soit en regard de causes (menaces) et de conséquences indésirables, auxquels l'exposition n'est pas formellement énoncée.

Dans plusieurs verbatims, le risque est considéré comme un danger auquel l'exposition n'est pas avérée (Magne 2010). Si l'on considère cette notion comme une menace potentielle il convient de la compléter par l'exposition à cette menace et la conséquence pour l'entreprise ou le dirigeant. Ce constat peut être mis en perspective à partir des verbatims suivants :

- *« …une **philosophie sécuritaire** pérennité de notre société […] on met en **péril** l'activité.. »*
- *« j'ai essayé de segmenter **les risques** »*
- *« … d'un schéma où il faut de temps en temps se mettre en faux **péril** […] c'est compliqué de se dire on va attendre **l'accident** »*
- *« … on a jamais eu de **gros problèmes** en huit ans d'existence »*
- *« … en 40 ans ce n'est pas arrivé et je ne vois pas pourquoi ça arriverait maintenant. Oui c'est un **risque hypothétique** »*

Ainsi, les risques énoncés seuls évoquent *« la perte », « le péril »* ou *« l'accident »*. S'ils indiquent une sensibilité du dirigeant comme une crainte d'un évènement indéfini, ils n'expriment pas l'aversion à l'évènement redouté. Effectivement, si Tsohou et al. (2006) mentionnent le risque comme concept abstrait car n'ayant pas de matérialité, un risque exprimé sans conséquence n'expose qu'une vision partielle de l'évaluateur et ne permet pas son évaluation. Nous appuyons la nécessité de considérer le risque non pas comme un concept abstrait (Tsohou et al. 2006) et complexe (Gerber et Solms 2005), mais comme une perspective d'un évènement redouté en regard d'une menace. En effet, rappelons l'immatérialité du risque souligné par Tsohou et al. (2006) qui, selon Kwon et al. (2013) le rend peu accessible, et la difficulté de considérer globalement les risques en regard de leur nature et leur diversité (Posthumus et Solms (2004). Le risque, s'il est défini comme un danger, ne permet pas d'accéder à ses caractéristiques fondamentales et d'élaborer une décision de traitement. En effet, le risque doit être contextualisé et exprimé pour sa finalité, la décision, ou, plus précisément, l'acceptation des risques (Yates et Stone 1992). Cette décision fait interagir une menace et des conséquences, avec une potentielle exposition à la menace (Fischhoff et al. 1978 ; Slovic et al. 1980) que nous développons ci-après.

Ainsi, les risques sont évoqués selon des **menaces** et des sources de menaces[68], telles des origines naturelles ou humaines, qui sont concordantes avec la littérature. Précisément, Loch et al. (1992 p. 176) évoquent 4 possibilités que sont la divulgation, la modification, la destruction et le déni de service, pouvant être causése intentionnellement ou par accident, par des sources[65] humaines ou naturelles, internes ou externes :

- *« … peut-être que je devrais couvrir **le risque de foudre** mais alors il faudrait que je couvre aussi le risque **d'inondation, d'incendie**, de… »*
- *« … s'il y a **un vol tout le matériel** pourrait disparaitre, comme pour **un incendie**, mais cela peut-être un **dégât des eaux** ce peut être tout… »*
- *« j'appuie sur les boutons pour **scratcher** les données j'y arrive… »*
- *« après on peut nous mettre **un virus** dedans pour que toutes nos données »*
- *« le **piratage** des données qui sont censées être confidentielles et internes se retrouvent plus ou moins publiques »*
- *« qu'il pourrait y avoir, en termes de **fuites** si on venait à capter notre base de photos*
- *« …dont on peut nous **piquer toute la gestion** »*
- *« On a eu 2 ou 3 fois des **attaques** sur notre site Internet »*
- *« …on s'est rendu compte que ce commercial **travaillait dans notre dos** »*

Cette approche du **risque par les menaces** renforce la notion de complexité du risque SI développé par Gerber et Solms (2005), entrainant une possible difficulté à « construire » un risque auquel il faudra répondre. D'autres commentaires confirment ce constat, par exemple *« C'est un poste ''fermé'' : il n'y a ni internet, ni rien, par sécurité…. C'est le cœur de mon métier, j'y ai tous mes clients, mes contacts. J'ai voulu que ce soit à part, qu'il n'y ait que moi qui ai accès… […] Et j'ai ressenti le besoin de vraiment séparer les activités. ».* Dans cet exemple, si l'on peut y voir *« Internet »* comme une menace, ce qui reste discutable et mériterait d'être approfondi, il n'apparait pas l'évènement redouté mais une volonté de *« séparer les activités »* en disposant d'un poste supplémentaire *« fermé ».* En ce sens, nous notons **les aspects techniques et technologiques sous-tendus** par les risques énoncés :

- *tout le monde **apporte des clés USB**, transmet des mails, les **postes ne sont pas forcément avec des anti-virus**, etc…*
- *j'ai essayé de segmenter les risques c'est-à-dire que je ne me suis pas mise … dans **une seule tour** pour réunir tout le monde.*

[68] Loch et al. 1992 indiquent des « responsables » (perpetrators)

- *… s'il y a **un vol tout le matériel pourrait disparaitre***
- *… mes **sites Internet seraient bloqués ou** sursaturés ce qui est plus classique…*
- *… la fiabilité du système informatique. **Pas l'information, l'informatique.** L'intrusion d'un virus qui me foutrait en l'air mon truc.*
- *…aujourd'hui, je me mets sur mon réseau, j'appuie sur les boutons **pour scratcher les données** j'y arrive !*
- *quelqu'un nous en voudrait il nous **enverrait un truc et on bousille** votre système…*

Dans ces exemples, si nous pouvons comprendre ou déduire l'évènement, par exemple, la perte de données ou de service pour *« le vol de matériel »* ou l'infection virale par l'*« apport d'une clé USB »* qui serait connecté au SI, nous n'en **voyons pas les conséquences pour « l'activité »** de l'organisation. Autrement dit l'énonciation de ces risques relèvent selon n**ous de la menace et non pas du risque**. En effet, la définition consensuelle du risque dans la littérature est plus complète car selon plusieurs auteurs le risque SI se définit par une **menace**, une **probabilité** et une **perte** (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Dhillon et Torkzadeh 2006 ; Sjöberg et al. 2004).

En regard de la littérature, l'énonciation technologique d'un risque SI soulève plusieurs commentaires. D'une part, **elle réduit la pertinence et la portée de l'analyse de risque**, de laquelle émergerait alors des mesures inadaptées aux problématiques réelles de l'organisation (Soomro et al. 2016). En effet, la vision techno-centrée des risques est décriée par plusieurs auteurs (Dhillon et Backhouse 2001 ; Karyda et al. 2005 ; Kayworth et Whitten 2010 ; Spears et Barki 2010). Précisément, ils suggèrent que **l'attention serait davantage portée sur des solutions immédiatement activables, ne laissant que peu d'espace à une réflexion globale sur la SSI**. En ce sens, rappelons la notion de solution optimale et de *satisficing* développée par March et Simon en (1958) et soulignée par Albrechtsen (2007) spécifiquement pour la SSI. Ces aspects techniques et technologiques des risques sont évoqués par plusieurs auteurs qui en expliquent l'approche. En effet Dhillon et Backhouse (2001) et Posthumus et Solms (2004) notamment, précisent que les SI relèvent du domaine technique inscrivant alors la SSI dans la perspective d'une problématique purement et uniquement technique[69].

Ainsi, les causes indésirables sont parfois clairement précisées. C'est ce que suggère l'extrait de verbatim suivant : *« **Le pire des risques** ce serait le **piratage des données** qui sont censées*

[69] Dhillon et Backhouse (2001 p. 132) étayent les raisons pour lesquelles la SSI est considérée comme technique à l'appui d'une traduction « mécaniste » des SI et des modèles qui en sont hérités.

être confidentielles *et internes se retrouvent plus ou moins publiques cela va être le pire des scénarios … ».* Si ce commentaire précise le risque en regard d'une menace (le piratage), la conséquence évoquée se révèle être la divulgation de données confidentielles. Pour autant, l'interviewé ne précise pas la **conséquence pour son entreprise et / ou pour lui d'un tel évènement,** soit la conséquence de la perte de confidentialité. Ce constat suggère alors que **le risque peut se définir selon une conséquence convenue universellement et implicite**. Convenue universellement car l'énonciation d'une divulgation de données révèle un risque dont la conséquence ne nécessite pas d'être évoquée. Selon nous, cette ellipse ne permet pas de satisfaire aux exigences d'évaluation du risque dans laquelle la conséquence n'apparait pas clairement et dont il faudrait en développer les impacts.

Notons que les menaces constitutives des risques considérés par les interviewés, apparaissent en accord avec les travaux princeps de Loch et al. (1992). Alors que Willison et Backhouse (2006) indiquent que la principale raison des faiblesses des dispositifs de sécurité des organisations est **leur défaillance à apprécier la valeur des ressources de leur SI** et les menaces auxquelles elles sont exposées, nos résultats montrent que **l'importance des SI est soulignée et justifiée par les dirigeants**, et que les **menaces sont, au moins partiellement, objectivées**.

Dans le prolongement des risques évoqués sans conséquences, nous abordons dans la section suivante les impacts possibles et l'exposition à ces risques.

6.1.3. Des conséquences considérées selon plusieurs perspectives

Les **conséquences** sont développées selon trois perspectives, les conséquences directes sur l'entreprise, les conséquences sur le dirigeant lui-même et les conséquences sur le « métier » supporté par le SI. En effet, rappelons que la littérature sur la SSI distingue ces « niveaux » de conséquences, permettant alors de les observer selon l'importance accordée par le décideur.

Les conséquences directes sur l'entreprise et sur le dirigeant

Les conséquences pour les dirigeants relèvent davantage des actions qu'ils auraient à conduire vis-à-vis de leurs collaborateurs telles que les placer *« immédiatement au chômage technique »* ou vis-à-vis de leurs fournisseurs ou clients (*« … même si les fournisseurs sont assez compréhensifs, c'était assez gênant pour moi de devoir les contacter pour leur dire de me*

renvoyer une base de prix parce qu'on ne l'a plus » et « *Quand vous devez appeler un client pour lui dire pouvez-vous me renvoyer votre bon de commande parce qu'on ne sait pas où il est passé…* »). Un dirigeant évoque *« une position de faiblesse »* vis-à-vis d'un fournisseur à qui il redemanderait le catalogue des prix. En effet, selon lui le fournisseur pourrait alors revoir les prix à la hausse et mettre l'entreprise « *commercialement »* dans « *une position de faiblesse ».*

Au-delà des conséquences pour les dirigeants eux-mêmes, soit pour **leur activité de manager,** les verbatims font émerger **la notion de responsabilité** qu'ils doivent assumer, telle que présentée dans la section ci-avant (6.1.1 « L'importance des SI au cœur du regard sur la SSI » p. 315). Rappelons que Mitchell (1995) décrit précisément la possible différence de perception des conséquences selon que le point de vue est celui du décideur pour lui-même ou pour son organisation.

En effet, les conséquences directes sur l'entreprise sont soulignées par les dirigeants qui relèvent notamment la perte de chiffre d'affaires et la pérennité de l'activité. Ainsi, lorsque la question est posée sur les conséquences qu'aurait une perte irréversible des données, il apparait une *« perte de CA* » de 20 à 30 % qui *« reste une estimation approximative* » tout en évoquant, dans le même temps, des conséquences bien plus importantes telles que « *je ne vais pas dire ''on ferme la boutique'' »* et *« je ne sais pas ce qu'il pourrait se passer… »* ou encore *« l'anéantissement de l'ancienneté et de tout ce que ça peut apporter dans mon activité, cela veut dire reparti à zéro… ».* Les conséquences pour l'entreprise sont également, dans un contexte peu favorable, évoquées comme indirectement causées par une perte de données, engageant une perte de temps dont le cout serait difficilement absorbable et mettrait en défaut la poursuite de l'activité (« … *mais ça peut être un coût de 30, 40 ou 50 K€ d'opérations en temps passé, en temps perdu à reconstituer. J'ai des données là-dedans qui sont tellement vieilles… aujourd'hui on fait 2 M€ de CA, donc 2,5% à 3% du CA […] parce qu'on est super tendus depuis des années et que c'est le genre de choses qui nous coûterait trop cher. »).* Ces verbatims montrent, sinon une connaissance des conséquences d'un risque SI qui impacterait l'activité de l'entreprise, les **conséquences ultimes possibles sur l'entreprise elle-même**. Ce constat peut être illustré par les propos de Kwon et Johnson (2014), qui indiquent par exemple, que la potentielle divulgation de données confidentielles aurait des conséquences directes sur l'organisation et ainsi indirectement sur les dirigeants.

Toutefois, si la littérature **établie une frontière** entre conséquences pour le dirigeant et conséquences pour son entreprise, **nos résultats montrent qu'elle est** tenue. En effet, dans les réponses des dirigeants interviewés, ces notions semblent se confondre. Nous pouvons dès lors mettre en perspective la perception des risques selon les conséquences majeures

pour les activités, sur le chiffre d'affaire et sur la poursuite même de l'activité l'entreprise, en regard de la responsabilité du dirigeant. Le verbatim le plus représentatif de cet engagement établit le lien entre perte, chiffre d'affaire et activité perdue : *« c'est mon entreprise donc je suis plus sensible à l'impact du chiffre d'affaires ou de l'activité perdue si ça m'arrive… »*.

Ainsi, la relation entre risque SI et considération des dirigeants constatée est en accord avec plusieurs auteurs. D'une part Moulton and Coles (2003 p. 580) soulignent la nécessité que « les directeurs identifient les risques "'informationnels" au **niveau de l'entreprise** ». D'autre part il apparait que ces dirigeants considèrent également la valeur de ces « **ressources organisationnelles critiques** » (Straub 1990 p. 255) que sont les SI. Les conséquences, défavorables et potentielles de ces risques, prises en compte par les dirigeants, s'inscrivent dans la nécessité de définir et de contrôler les processus de gestion des risques et de mise en œuvre des contre-mesures, dont ces dirigeants ont, *in fine*, la responsabilité (Moulton et Coles 2003 ; Posthumus et Solms 2004 ; Solms 2001a ; Straub et Welke 1998). Ces conséquences sur le dirigeant et l'entreprise peuvent alors **matérialiser une influence prégnante pour la SSI**, telle que l'indiquent Posthumus et Solms (2004) ou précisément Solms (2006) pour qui l'engagement de la gestion des risques est fondamental en SSI.

À un autre niveau que celui du dirigeant et de l'entreprise, nous constatons que les conséquences évoquées peuvent avoir un impact sur le métier.

Les conséquences « métier »

Les conséquences « métier » des risques pesant sur SI touchent davantage l'économie, l'image ou la désorganisation. Ce sont ces catégories de pertes qui émergent de nos verbatims avec des articulations entre elles, parfois sous-tendues ou qui apparaissent directement.

La **perte de temps** est liée, dans le verbatims, à une **perte de données** qui sont supprimées ou qui ne peuvent être recouvertes et qui sont essentielles au fonctionnement de processus métier. Ainsi, les dirigeants évoquent *« l'incapacité de travailler sur une demi-journée »* qui rend le fonctionnement de leur organisation *« compliqué »* parce qu'ils *« perdent du temps ».* Ils évoquent une perte de données liée à un évènement qui entraine *« la perte totale de ce qui a pu être fait entre la dernière sauvegarde et le moment de l'accident ».* Aussi, l'impossibilité de facturer implique une perte de temps pour reconstituer les données *(« Et les clients aussi parce qu'on a perdu aussi une semaine de travail sur tout ce qui était devis et facturation. »).* **La**

dépendance à des services informatiques externes est aussi abordée, en ce sens où elle implique un arrêt de l'activité des dirigeants lorsque le prestataire faillit *(« Quand on **perd la connexion …, je ne peux plus travailler** »* et « *…on réinstalle et je dis au prestataire : ''vous me refaites la redescente !*'' (des données)*… La dernière sauvegarde elle avait 3 mois chez eux … ».* En ce sens, les services du prestataire peut être justement prévus pour pallier une défaillance quant à la disponibilité des données (*« …j'appellerais mon prestataire en lui demandant comment cela est possible sachant tout ce qui me coûte, je lui paye un antivirus, un machin et voilà j'attends ça de mon prestataire et sinon je restaurerais les informations de la veille et au moins je n'aurais perdu que le delta »).*

Ces pertes sont parfois traduites **en pertes financières** qui sont décrites comme indirectes. Ainsi, le **vol de la base de données** des clients de gestion locative aurait pour finalité, pour l'auteur du méfait, de récupérer les contrats à son profit (*« quelqu'un pourrait essayer de travailler avec le propriétaire …donc si vous avez facilement accès à cette base vous pouvez les contacter vous savez les gens qui démarrent peuvent proposer un tarif plus bas que le mien en faisant valoir l'intérêt pour le client »).* Le coût d'un incident s'exprime aussi en termes de **perte de temps** avec pour conséquences « secondaires » **des pertes financières** *« … un coût de 30, 40 ou 50 K€ d'opérations en temps passé, en temps perdu à reconstituer. J'ai des données là-dedans qui sont tellement vieilles ».* La perte financière peut aussi être causée par un défaut de **respect de la réglementation**, notamment sur les données médicales et personnelles. Ainsi, *« une réglementation un petit peu particulière qui concerne la protection des données médicales »*, qui peut impliquer « *une amende par questionnaire »* car *« on a 900 questionnaires de santé et l'amende peut aller jusqu'à 150 € par dossier ».* Pour une activité traitant de données médicales, au-delà de la réglementation spécifique, sont des évoqués des *« risques multiples »* soit des risques impliquant des conséquences triple, financière, d'image et juridique : « *…sur le plan financier 4 % de notre chiffre d'affaire en cas de non-respect de la règle c'est énorme très clairement et aussi un risque pénal nos patients peuvent nous attaquer si on a pas fait en sorte d'assurer la confidentialité de leurs données, les risques sont multiples… »*. Spécifiquement à la nature des données et à un risque dont les conséquences sont multiples, ce constat est relevé par Kwon et Johnson (2014 p. 455). Pour ces auteurs, la sensibilité du public à la divulgation de donnés médicales privées provoque « souvent des réactions exceptionnellement fortes ». En effet, ils précisent que la réglementation crée une pression double, obligeant la déclaration des incidents auprès des organisations de contrôle et des patients, exposant alors l'organisme médical à une potentielle perte d'image auprès de ces derniers et pouvant conduire à des condamnations sur le plan pénal.

Ensuite, ces pertes sont parfois traduites en **termes de désorganisation** , conséquence possible de la perte de données et de temps. Il peut s'agir de la perte de données spécifiques telles que des mails (*« … et donc depuis 6 mois, les mails n'étaient pas sauvegardés. Et donc, si on avait eu un clash à ce moment-là […], on n'était pas capables de ressortir les mails. Ça pose le problème de faire et de vérifier ce qu'on a fait. »*) qui peuvent mettre en défaut l'entreprise quant à la traçabilité des ordres formalisés et qui pourraient alors être reprochés au dirigeant, précisant que la conséquence redoutée **relève davantage d'une conséquence liée à la perte de la donnée**. En ce sens, d'autres verbatims montrent les conséquences induites par la perte de données, qui sont *« découvertes au fur et à mesure »,* à l'origine d'une désorganisation ou d'une obligation de reconstruire ses données durant *« trois à quatre mois de l'année »,* impliquant l'absence *« d'extension »* et *« croissance sur le plan financier… ».* Ces conséquences « désorganisantes » sont également évoquées lorsqu'il s'agit d'une conséquence de perte de données liée à un incendie (« …*j'ai quelqu'un qui me brûle tous mes cabinets. Normalement, avec un ordinateur, je suis censée pouvoir récupérer toutes mes données. »)* et d'une impossibilité de recouvrir l'ensemble des données perdues *(« je me dis qu'au pire on perdrait, parce qu'on perdrait forcément, j'ai du mal à croire qu'on restaurerait tout immédiatement, 1 semaine, 2 semaines, 3 semaines de boulot… »).*

Enfin **les pertes d'image** sont également mentionnées. Dans le respect des principes des pertes évoquées ci-avant, la perte d'image est souvent une conséquence d'une perte de service ou de données. Ainsi, on constate une dépréciation de l'image suite à un site Web qui ne permet pas au client de réaliser ses commandes **(*« quand un site est ralenti c'est pénible et donne une mauvaise image, quand le service client ne répond pas, on a une mauvaise image… »***). La diffusion d'information par des tiers, suite à une perte de confidentialité renforce que la conséquence redoutée n'est pas tant la perte de confidentialité que la divulgation des données pour lesquelles le besoin de confidentialité a été mise en défaut. En ce sens, le vol de données médicales est redouté par une possible conséquence d'un usage malveillant de ces données « *qui était dans ce SI parce qu'à l'époque le dossier patient n'était pas informatisé… »* alors que *« dans le dossier administratif, il y a des données nominatives de patient... ».*

Les commentaires des dirigeants interviewés sur les conséquences possibles sont **concordants avec celles évoquées dans la littérature portant sur la perception des risques et/ou sur la SSI.** Pour la perception des risques, rappelons que Yates et Stone

(1992) définissent une taxonomie de perte[70] qui mentionne, notamment, les pertes financières, les pertes de performance, les pertes physiques et les pertes de temps. Dans le champ de la SSI, ces conséquences possibles précisent, des **dysfonctionnements** impactant l'activité des métiers supportés par le SI (Bandyopadhyay et al. 1999 ; Doherty et al. 2011), une **dépréciation de l'image** ou des **implications juridiques** pour l'organisation (Dhillon et Torkzadeh 2006 ; Höne et Eloff 2002b ; Kwon et Johnson 2014), des **arrêts de production** (Doherty et Fulford 2006 ; Posthumus et Solms 2004 ; Straub 1990), des coûts de rétablissement du SI, des **pertes financières directes** (Bagchi et Udo 2003 ; Choobineh et Dhillon 2007) ou indirectes (Bagchi et Udo 2003 ; Choobineh et Dhillon 2007 ; Ma et al. 2008), des pertes **économiques ou financières** (Bandyopadhyay et al. 1999 ; Baskerville 1993 ; Cavusoglu et al. 2004).

Nous **prolongeons alors le champ des conséquences possibles** pour les risques SI par **la désorganisation et la perte de temps** pouvant succéder un évènement qui met en défaut la sécurité du SI. Notons que ces deux conséquences sont évoquées par plusieurs dirigeants comme conséquence directe ou indirecte. Si, dans le champ de la SSI, la **perte de temps** n'est pas mentionnée, elle l'est dans le la discipline psychologique de la perception des risques, notamment par Yates et Stones (1992). Nous pouvons mettre ces résultats en perspective de la proximité du dirigeant avec les activités métier de son organisation et les conséquences qu'il constaterait directement compte tenu de l'organisation de son entreprise et de leur taille, comprise principalement entre 2 et 20 collaborateurs dans une structure faiblement pyramidale. Lorsqu'il s'agit d'une organisation plus complexe, nous pouvons inférer que des évènements opérationnels seraient traités par plusieurs strates de l'organisation avant d'être communiqués au comité de direction au travers de « structures organisationnelles appropriées » (Solms 2006 p. 167). **La désorganisation** n'est pas mentionnée dans le champ de la perception des risques. De plus, en ce qui concerne les travaux en SSI, seules les recherches de Ma et al. (2008 p. 252) évoquent « la perturbation de processus internes » pouvant signifier une conséquence possible sur l'organisation de l'entreprise. **Les constats que nous avons établis renforcent donc cette conséquence possible d'un risque SI**.

L'ensemble des constats sur les conséquences mettent davantage en exergue la **complexité des conséquences relevées** par Gerber et Solms (2005) et la difficulté de les évaluer globalement sur plusieurs plans (Slovic 1992). En ce sens, rappelons la subjectivité et la

[70] Voir le détail de cette taxonomie au chapitre 3.2.2 Concepts de l'étude des risques p. 111 dans la section « les conséquences »

contextualité du risque qui selon Kermisch (2012 p. 5) « n'est pas considéré comme quelque chose d'extérieur que l'on peut percevoir » indépendamment de son contexte, pour les individus comme pour les organisations. Si Yates et Stone (1992) précise que l'évaluation du risque consiste à déterminer les pertes potentielles ils soulignent la divergence des catégories[71] des conséquences prises en compte pour un même risque. En effet, ces catégories sont situationnelles et se distinguent des caractéristiques du risque de Slovic et al. (1984, qui définissent 16 items tels que par exemple la volonté de s'exposer au risque, le contrôle possible sur le risque, la familiarité du risque…). L'exemple de Yates et Stone (1992) nous semble le plus représentatif pour illustrer **l'incertitude de catégorie**. « Jane Smith » définit ses attentes pour son futur emploi selon trois catégories écartant une quatrième catégorie que serait la potentielle source d'inconfort provoqué par ses futurs collègues de travail. C'est donc le choix d'un emploi dans lequel Jane Smith perçoit cette quatrième catégorie qui l'éclaire sur une conséquence qu'elle n'avait alors pas considérée.

L'heuristique de **représentativité**, qui consiste à rattacher la situation à évaluer à une classe ou schéma selon la définition d'Amalberti (1996), peut aussi conduire à ne pas représenter l'ensemble des catégories possibles et non désirées (Hermand et Chauvin 2008 ; Slovic et al. 1982 ; Yates et Stone 1992). Rappelons également que l'absence d'une approche holistique des conséquences est évoquée par Slovic et al. (1979 ; 1984). Ainsi, la subjectivité, la contextualité et l'incertitude des conséquences contribuent à la **difficulté d'aborder des conséquences qui sont parfois indirectes.** Ce constat est corroboré par Cadet et Kouabénan (2005), pour qui les conséquences peuvent être multiples et variées et dont il n'est pas certain que l'évaluateur puisse imaginer et en définir l'ampleur (Slovic et al. 1979).

Straub et Welke (1998) citent Loch et al. (1992 p. 183) pour qui « beaucoup d'organisations sont sous-sécurisées, beaucoup de managers continuent à ignorer la question et à être "naïfs" dans leurs réponses au défi posé par cette menace croissante ». Notre analyse des verbatims fait émerger la complexité d'évaluer les risques, notamment par une approche parcellaire de ce dernier, sous l'angle des menaces ou des conséquences. **Cela ne converge pas avec l'approche des travaux du paradigme psychométrique** qui nécessite d'objectiver les risques par leur conséquences et leur probabilité de survenance, afin de prendre une décision quant à l'acceptation du risque, soit la finalité de leur « gestion » (Cadet et Kouabénan 2005 ; Fischoff et al. 1981 ; Kermisch 2010 ; Slovic et al. (1979 et 1982).

[71] Les catégories de risques de Yates et Stones (1992) sont précisées dans la section « Le risque acceptable » p. 114

En ce sens, les thèmes « gouvernance » et « analyse de risque » de la littérature SSI donnent une perspective particulière sur la **faible perception des risques SI des top-managers**. Selon les tops-managers, il n'est pas toujours nécessaire d'élaborer un dispositif de sécurité car les SI sont faiblement **exposés aux risques** (Kankanhalli et al. 2003).

6.1.4. Une exposition à la menace peu objectivée

L'évaluation du risque, comme nous l'avons abordée et telle que précisée dans la littérature, nécessite de considérer la menace et les conséquences ainsi que la probabilité de survenance de ce risque. Selon plusieurs auteurs en SSI, il s'agit alors, pour les dirigeants, de disposer d'une vision globale des risques SI qui pourraient mettre en cause le fonctionnement des activités et provoquer des impacts sur la société (Kwon et al. 2012 ; Soomro et al. 2016 ; Straub et Welke 1998). Aussi, dans le champ de la recherche en psychologie, l'évaluation du risque nécessite d'aborder, **dans le même temps**, l'ampleur des **conséquences** d'un évènement indésirable et leur **probabilité** de survenance (Amalberti 1996 ; Hermand et Chauvin 2008 ; Cadet et Kouabénan 2005 ; Slovic et al. 2004 ; Sjöberg et al. 2004).

Si les verbatims sont denses lorsqu'il s'agit de décrire les menaces, ils ne relèvent que peu **l'objectivation des probabilités** de risque par les dirigeants. Selon nous, cette notion apparait toutefois dans les verbatims, non pas sous la forme de potentiel de survenance du risque ou d'exposition aux menaces mais telle une **prise de conscience de l'existence d'un risque** et d'y être exposé, ou à l'inverse, de ne pas y être exposé.

Ainsi certains dirigeants annoncent, à la lumière des mesures de sécurité qu'ils ont définies, qu'*« il y a toujours un petit risque »* tout en minimisant leur exposition car, ils ne pensent pas être *« une multinationale »*, *« ne pense pas être la cible numéro 1 »*, et bien qu'il ne soit pas à *« l'abri »* parce que « *ce n'est pas particulièrement peu sécurisé », assurent que « ce n'est pas une banque »* sous-entendant la faiblesse du potentiel risque. Un autre dirigeant[72], dans la même phrase, s'interroge sur la pertinence « de *tout avoir au même endroit ! »* lorsqu'il parle des postes et de ses sauvegardes, diminuant ainsi son niveau de sécurité en cas de vol ou d'incendie par exemple, pour indiquer qu'il a *« l'impression qu'on* (il) *est un peu dans le minimalisme, dans l'amateurisme »* et de conclure par : *« on fait le minimum mais j'ai l'impression qu'en fait on couvre assez bien notre sujet, notre sauvegarde. ».* Selon nous, ces propos sont en accord avec la littérature sur la perception des risques. D'une part, Slovic et

[72] D2

al. (1979) soulève la difficulté d'évaluer la probabilité d'un risque pour lequel peu ou pas de données significatives sont disponibles, empêchant un calcul probabiliste de survenance. Cette difficulté renforce l'incertitude sur la réalité même du risque car dépendante d'une existence attendue comme incertaine par le décideur (Yates et Stones 1992). Notons que tous ces commentaires convergents vers la nature du risque, contextuel et subjectif. En ce sens, Slovic et al. (1982a) inscrivent le risque comme un **objet social attendu** qui n'est perçu que par ses évaluateurs en regard de déterminants sociaux. La difficulté d'estimer la probabilité de ces risques corrobore ainsi les propos de Fischhoff et al. (1978) et Slovic et al. (1980), « écartant de la vue ce qui est en dehors de l'esprit » dès lors que le risque n'a pas encore été vécu. Ceci peut porter un éclairage nouveau sur les commentaires de plusieurs auteur en SSI qui soulignent l'absence de considération pour les probabilités (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Taylor 2006). Rappelons que Taylor (2006 p. 1585) évoque la « cécité des exécutifs » développée par Slovic et al. (1987) pour justifier que les top-managers « ont tendance à avoir une **perception incorrecte** des événements **en ignorant les probabilités** et utilisant à la place des mécanismes heuristiques ».

Si cette « cécité » peut sembler avérée avant un risque vécu, le risque apparait clairement dès lors que les top-managers y sont **directement confrontés**. Si un dirigeant[73] s'appuie sur l'absence d'évènement et un chiffre d'affaires « réduit » selon lui, pour justifier la faible probabilité du risque SI, un incident « bloquant » et « impactant » l'oblige à réviser son évaluation (*« en 40 ans ce n'est pas arrivé et je ne vois **pas pourquoi ça arriverait maintenant**. Oui c'est un **risque hypothétique** »* et *« Pour moi, je ne voyais pas qui pourrait nous hacker : notre société fait 1 million de CA max, on ne pèse rien. Sauf que je n'avais pas pensé au ransomware »*). Cette révision « forcée » des probabilités est décrite par Slovic et al. (1984 p. 200), qui indiquent que seuls les risques dont les conséquences dépassent celles imaginées par l'évaluateur sont considérés. Autrement dit, un risque devient « probable » lorsque sont objectivées des conséquences « de grande ampleur » (Cadet et Kouabénan 2005 p. 28). Slovic et al. (1984 p. 200) développent ce constat en précisant que les croyances et connaissances d'un risque par un évaluateur sont « impactées » dès lors qu'un accident a des conséquences qui ne sont pas familières ou est issu d'un dysfonctionnement qui n'est compréhensible, ce qui semble être le cas de la situation décrite dans nos verbatims.

Cela étant, un des dirigeants présente une approche sensiblement différente de sa perception à l'exposition au risque. En effet, il s'appuie sur l'absence de problème durant les 8 années d'activité et la faible visibilité de son entreprise, conformément aux verbatims précédents,

[73] D3

pour justifier qu'il n'est pas exposé au risque : « *… je touche du bois on a jamais eu de gros problèmes en huit ans d'existence […] on fait de l'espionnage donc par définition y'a que James Bond qui est un espion qui se fait voir, nous on est plutôt en mode discret donc je pense que ça joue… ».* **Bien qu'il ait rencontré deux risques** (liés à une perte de disponibilité et menace d'un ancien collaborateur sur une potentielle perte d'intégrité), il déclare être *« plus intéressé par les pratiques de sécurité de sa* (ma) *voiture »* que de sa société. Nous pouvons alors mettre en perspective sa position en regard de la faiblesse des impacts des risques vécus, dont Slovic et al. (1984) précisent qu'ils ne sont pas assez conséquents pour remettre en cause la « réalité du risque ». Autrement dit, les **conséquences vécues par ce dirigeant ne sont pas assez importantes** pour qu'il s'attache à les analyser et y remédier. Une autre perspective peut aussi émerger de ces propos. En effet, son SI s'appuie notamment sur un prestataire dont il loue les compétences techniques et qu'il décrit comme *« un grand spécialiste de la sécurité en France »*. Ces constats peuvent renvoyer à la vision technique de la SSI, puis, articulée à la faible exposition perçue, à la notion de contrôle. En effet, la vision technique est décriée par Willison et Backhouse (2006) qui pointent l'absence de relation entre fonctions métiers et sécurité, conduisant à mettre en place des mesures inopportunes ou inefficaces et créant alors une **fausse impression de sécurité**. Ensuite, la notion de contrôle sur le risque, développée par Cadet et Kouabénan (2005) et Chauvin et Hermand (2006) consiste en une diminution de l'exposition perçue **dès lors que les évaluateurs estiment contrôler la situation**. Précisément, rappelons que Peretti-Watel (2000), souligne un niveau de maitrise perçu par l'évaluateur supérieur à celui des autres, le conduisant à penser contrôler le risque et par conséquence à y être moins exposé. Ensuite, pour une situation où l'activité est génératrice de biens mais aussi de possible nuisances, plusieurs auteurs ont démontré le **rôle de l'affect** (Alhakami et Slovic 1994 ; Finucane et al. 2000 ; Slovic et al. 2004). En effet, la prise en compte de deux dimensions, probabilités et appréciation de l'utilité des conséquences, comme composantes de l'évaluation, amène à définir le risque acceptable[74] comme une référence à une valeur intermédiaire entre avantages et conséquences négatives (Fischoff et al. 1981). Ainsi, pour ce dirigeant, cette approche triple de son exposition peut éclairer sa perception du risque potentiel malgré les risques vécus ou éviter de justesse.

Les perceptions des risques observées corroborent les propos de Bandyopadhyay et al. (1999 p. 440) indiquant une décision pour le risque SI qui diffère « des concepts théoriques » et qui écarte « l'évaluation des probabilités de résultats possibles ». Ce constat est

[74] Dans ce cas le risque « brut » est acceptable et ne nécessiterait pas d'être couvert par des mesures de sécurité

convergeant avec les travaux sur les risques SI et ceux abordés dans le champ psychologique de l'évaluation des risques. En effet, si une réalité des risques SI est possible, l'évaluation de ces possibilités n'est pas formelle. Ce constat rappelle à nouveau la subjectivité du risque et la difficulté d'en évaluer son exposition, telle que décrit dans la littérature, qui confirment que la décision pour le risque est davantage **centrée sur l'ampleur des conséquences négatives** que sur **l'incertitude de survenance de ce risque** (Yates et Stones 1992). En prolongement de ce constat, Loch et al. (1992 p. 185) émettent l'hypothèse sur l'explication de ce dernier constat par la **« croyance plutôt naïve que de mauvaises choses arrivent seulement aux autres** ».

Après avoir abordé la possible prise en compte des menaces et les conséquences dans la décision pour le risque SI, nous pouvons en détailler l'origine de la connaissance des dirigeants.

6.1.5. Différentes sources pour la connaissance des risques SI

Slovic (1992 p. 5) rappelle que la supposition première du paradigme psychométrique est « que le risque est intrinsèquement subjectif » et qu'il « n'existe pas indépendamment de nos esprits et cultures ». Ainsi, l'évaluation repose « **sur des inférences fondées sur ce dont ils se souviennent, ce qu'ils ont entendu ou observé à propos du risque en question** » (Slovic et al. 1979 p. 15). Les interviewés sont informés des risques par des sources d'origines différentes mais non exclusives que nous discutons dans cette section.

La première source d'information sur les risques relève, presque « naturellement », de **l'expérience vécue**. Selon nous le verbatim le plus représentatif de cette idée est porté par un dirigeant qui a subi les conséquences d'un ransomware « *Je pense que je n'avais pas du* ***tout conscience*** *de ce que cela pouvait impliquer. Quand on a été touchés par le ransomware, ça nous a bloqué tout le serveur… on a perdu tous les fichiers qui étaient sur le serveur* ». D'autres dirigeants ont vécu des expériences comparables, de perte de confidentialité et de perte de donnée, soit pleinement subies soit évitées de justesse « *… on a scanné pendant trois jours quelque chose qui ne s'est jamais sauvegardé …mais ça nous a fait* ***prendre conscience*** *qu'il fallait peut-être sauvegarder les données parce qu'on s'est dit que* ***si on venait à perdre des jours des jours des jours comme ça … ce serait des milliers d'heures de perdues »*** ou *« quand j'ai pris conscience de ça, je me suis dit qu'il fallait protéger nos informations des* ***risques qui pouvaient nous tomber dessus*** ». Ces risques dont les dirigeants ont vécu la

survenance et la conséquence, s'inscrivent parfaitement dans la littérature sur la décision de traiter des risques, tant dans le champ psychologique (Slovic et al. 1979) que celui des SI (Choobineh et al. 2007), indiquant que les risques sont considérés dès lors qu'ils **sont connus** et **qu'ils peuvent concerner le décideur**. En ce sens, Kermisch (2012 p. 1) évoque une subtilité intéressante en faisant valoir que « lorsqu'un risque se matérialise, il ne s'agit plus d'un risque mais **d'un sinistre** ».

Une seconde source d'information sur les risques apparait **dans les échanges avec les réseaux d'influence** propres aux dirigeants ou **aux communications des médias**. Ces réseaux d'influence concernent autant les proches que les prestataires, ou les associations professionnelles auxquelles les dirigeants adhèrent. Ainsi, plusieurs évoquent la connaissance de *« quelqu'un qui râle parce qu'il a perdu les données »* ou des *« échanges avec des gens de cercle proche ou moins proche d'ailleurs qui vont vous raconter une expérience malencontreuse »*. Les risques communiqués dans ce cadre relèvent essentiellement de la perte de données ou du piratage.

La perte de données la plus représentative de nos verbatims est énoncée par un dirigeant qui *« crois qu'il y a une transmission d'angoisse… »* transmise par ses fournisseurs et prestataires, qui le conduit à conclure *« ce serait vraiment dramatique effectivement de perdre des données ».* En outre, les autres communications à l'endroit des dirigeants sont établies non par sur le risque mais sur **menaces exclusivement** telles que par exemple :

- *« … des voisins, partenaires, amis qui se font **piquer leurs données** »*
- *« … un ordinateur qui **tombe en panne** »* et *« … des choses qui arrivent à des copains qui perdent un **disque dur qui a cramé** … qui perdent le contenu de leur téléphone… »*
- *« … c'est l'actualité : un **cambriolage** »*
- *« des bâtiments qui **avaient brûlé**, des vols, des choses comme ça… »*
- *« …il y a plusieurs des écoles […] qui se sont fait d**étourner des informations** ! »*
- *« ..le journal télévisé où tu entends ces histoires de **piratage** et de demande de rançons. »* et *« on entend parler de plus en plus de **ransomware »***
- *« je fais **partie d'un club où il y a régulièrement** des **gens qui informent** les autres sur **les risques** … »*

On constate que ces risques sont **communiqués sous le seul angle de la menace**, qu'elle relève de l'action malveillante « volontaire » au sens de Loch et al (1992) telle le vol ou le piratage, ou involontaire telle l'incendie ou la panne technique. Précisément émerge de nos

verbatims une connaissance centrée sur la **perte de données** quelle que soit la menace évoquées.

En regard de ces constats, nous réitérons le commentaire de la section 6.1.2 « Des risques souvent définis partiellement » (p. 318), à savoir que le risque ne peut s'objectiver seulement en regard des menaces mais doit être considérer selon son exposition et ses conséquences. Ces commentaires peuvent renforcer l'impossibilité de concevoir le risque comme « quelque chose d'extérieur que l'on peut percevoir » (Kermisch 2012 p. 5) et pour lequel il y aurait un **consensus sur ces impacts et son exposition indépendamment de l'activité et de son contexte**. En effet, (Kermisch 2010) met en évidence dans l'étude du paradigme psychométrique du risque la convergence de certains déterminants entre plusieurs évaluateurs, indépendamment d'un réel consensus le niveau global de risque. **Autrement dit, si la menace peut se traduire différemment dans la conceptualisation de plusieurs évaluateurs, il y a consensus sur la menace elle-même**.

En ce sens, nous observons que les échanges **suscitent une réflexion sur la propre protection du SI** telles que *« des échanges avec des gens de cercle proche ou moins proche d'ailleurs qui vont vous raconter une expérience malencontreuse et où on se dit il aurait pu m'arriver la même chose, je n'aurais pas été mieux loti et donc on **peut essayer de s'en préoccuper**, »* ou encore, plus directement, la question *« et moi, si ça m'arrivait demain, **comment je gère** ? ».* Parmi ces *« gens de cercle proche »* se trouvent *« des particuliers et des professionnels »* dont les dirigeants sont *« à l'écoute de ce qui se passe et des expériences »* et des *« mauvaises histoires »* qui vont être utilisées pour identifier si ces évènements peuvent leur arriver et comment ils pourraient faire pour y remédier, soit un processus de décision en accord avec la gestion et l'acceptation du risque développées dans le champ de la recherche en psychologie (Fischoff et al. 1981 ; Slovic et al. 1979, 1982, 1987).

En synthèse, rappelons que la gestion des risques et l'acceptation des risques, font interagir notamment les bénéfices perçus, le contexte et les enjeux de la situation risquée (Sjöberg et al. 2004 ; Yates et Stone 1992).

6.1.6. Connaissance « isomorphique » des risques et de la SSI

Nous avons développé, dans les sections précédentes, les influences possibles sur la connaissance du risque et de la SSI. Nous prolongeons notre discussion des résultats selon les influences isomorphiques, quelles soient normatives, coercitives ou mimétiques. Rappelons que ces influences peuvent relever de l'effet des réseaux d'influence, des effets de la loi ou de la réglementation et les effets de l'adoption des pratiques d'un concurrent.

Les premières **influences normatives** que nous avons identifiées émergent de l'adoption de pratiques professionnelles, choisies pour répondre à de possibles mises en cause sur le plan de la réglementation. Il s'agit alors d'assurer la remédiation de deux risques : le risque pouvant impacter le SI et le risque induit par l'absence de réponse à une exigence réglementaire. Afin d'éviter ces deux risques, les dirigeants, qui ne sont pas nécessairement des spécialistes de ces deux domaines (McFadzean et al. 2007), doivent alors s'attacher à y répondre, pouvant les conduire à échanger sur ces pratiques en l'absence de solutions accessibles pour les mettre en œuvre (Di Maggio et Powell 1983).

Ainsi plusieurs dirigeants, devant le manque de connaissance pour ces pratiques, appellent à se renseigner auprès de **professionnels**. L'absence de connaissance est aussi évoquée comme un problème lié à la difficulté d'appliquer les règles RGPD telle qu'illustrée par les verbatims : *« on pourrait avoir un client qui viennent nous voir au bout de six mois et qu'il me dise ''vous avez gardé les données .., je vous ai envoyé un mail comme quoi il fallait les supprimer …et vous ne les avez pas effacées'' »*. Spécifiquement aux pratiques observées pour la SSI, cette influence est directement traduite par le prestataire informatique qui propose une mesure de sécurité qu'il met lui-même en œuvre.

Nous constatons que cette influence normative concerne autant le « partage de croyances » sur les risques, issues de l'appartenance à des groupes au sens de Douglas et Wildavsky (1982), que d'adoption de pratiques de SSI, issues de réseaux associatifs ou professionnels au sens de Scott (1995). Douglas et Wildavsky (1982) précisent que l'**appartenance au groupe** met en évidence des perceptions de risques partagées autour de croyances, de valeurs et attitudes communes. La verbatim qui illustre le mieux ce constat relève de la transmission de la « suspicion » : « *Mon père effectivement étant policier m'a toujours transmis de toujours faire attention… »*. La transmission de la solution est davantage relevée par un autre dirigeant qui met en œuvre les pratiques de son père *(« Je prends l'exemple de mon papa qui faisait des sauvegardes »)* s'inscrivant alors dans une pratique mimétique.

L'adoption de pratiques de SSI est influencée par les échanges dans les réseaux associatifs et particulièrement par les professionnels prestataires des dirigeants (Scott 1995 ; Williams et al. 2009). On relève ainsi que les dirigeants se satisfont des connaissances sur les risques et les pratiques issues de leur syndicat (*« on a un très bon syndicat : il fait de la veille réglementaire »)* ou de leur club (*« …un club où il y a régulièrement des gens qui informent les autres sur les risques »*). Si ces échanges peuvent alors faciliter la diffusion de connaissances sur les pratiques exercent également des pressions normatives (Di Maggio et Powell 1983), ils peuvent aussi contribuer à l'élaboration d'une culture commune du risque (Cadet et

Kouabénan 2005) que nous relevons dans les propos d'un dirigeant qui précise *« qu'il y a une transmission d'angoisse »*. En prolongement de ce constat les prestataires semblent justement avoir un double **rôle pour l'influence** sur les **pratiques** et sur les **risques**. Ainsi, un dirigeant regrette ne pas avoir souscrit à une recommandation de son *« prestataire informatique »* qui lui a indiqué une bonne pratique sur la sauvegarde, alors qu'un autre est conseillé par un prestataire qui « minimise » les risques (« *Elle a été un petit peu plus dans la minimisation des risques plutôt que de mettre en perspective les potentiels problèmes qu'il pourrait y avoir, souvent elle disait qu'il y avait des choses dont on avait pas besoin en précisant qu'avant qu'il arrive ça ou ça, il va s'en passer... ».* Enfin, on constate aussi un accompagnement technique durable de ces prestataires qui participent aux décisions quant à la SSI (*« … la sécurité, enfin les postes informatiques en eux-mêmes, j'ai dans mon historique mon premier prestataire informatique avec qui on a beaucoup échangé »).* On constate dans nos verbatims une articulation des influences normatives et mimétiques, en accord avec les conclusions de Williams et al. (2009), qui, rappelons-le, ont démontré que l'adoption de mesures de sécurité peut être influencée par les effets de la combinaison de pressions normatives internes et externes, de pressions mimétiques et de pression coercitives.

Les **pressions institutionnelles coercitives** prennent souvent la forme de lois ou de règlements et revêtent un caractère incontournable pour les organisations qui y sont exposées (Scott 1995). Les influences coercitives constatées s'inscrivent particulièrement en regard de la réglementation sur la protection des données personnelles ou plus spécifiquement de règlementation particulière. Nous retrouvons alors le caractère obligatoire dans les verbatims des dirigeants qui précisent : *« …je sais qu'il y a la fameuse loi RGPD. Donc nous, au sein de l'entreprise, on est sensibilisés à ça auprès de nos clients et on doit rentrer dans les clous ».* Cependant, nous constatons que l'obligation de respecter ces règles n'est **pas nécessairement une influence sur la réponse au risqu**e ou sur l'adoption de la SSI. En effet, si plusieurs dirigeants évoquent la sanction en cas de non-respect (*« 150 € par dossier »* ou *« perte d'agrément »*), ils font valoir dans le même temps la conséquence de risque, dont certains relèvent de ces réglementations, ou ne les respectent pas toujours : *« les risques sont multiples … avez le RGPD sur le plan financier, 4 % de notre chiffre d'affaire en cas de non-respect de la règle… et aussi un risque pénal, nos patients* ***peuvent nous attaquer*** *si on a pas fait en sorte d'assurer la confidentialité de leur données.. ».* Un autre dirigeant, lui aussi soumis à une réglementation sur la protection des données, se **savait en défaut *« en connaissance de cause****, comme 90 % des structures »*. C'est la potentielle perte de données qui lui *« a fait prendre conscience qu'il fallait peut-être sauvegarder les données ».* D'autres

verbatims confirment ces propos, appelant la protection des données, selon le risque vécu et la nécessité de répondre à la réglementation : *« Certains l'ont fait pour protéger leurs données nominatives et parce que la loi l'exigeait et d'autres parce qu'ils ont eu un vrai problème ! »*. Dans cette ligne, un dirigeant ne **respecte pas une réglementation** spécifique qui lui est imposée et ne perçoit pas les risques qu'elle prévoit de couvrir, pensant notamment qu'il *« …ne risque pas grand-chose avec le brave monsieur*[75] *là mais voilà… »*.

Ainsi, si les influences coercitives appelant la gestion du risque ou la SSI sont sous-tendues dans les verbatims, il ressort qu'elles ne sont pas toujours respectées et **se situent sur un second plan par rapport au risque SI**. En effet, les dirigeants **semblent être plus intéressés par les conséquences** et attachés à couvrir les risques plutôt qu'à considérer la règlementation et ses implications. En ce sens, Williams et al. (2009) souligne la combinaison de pressions coercitives et normatives qui ne s'observent pas unitairement, mais davantage comme des moteurs combinés pouvant conduire à l'adoption de mesures de sécurité. Précisément, l'adoption de ces mesures a été réalisée sur une période de temps articulant les interactions et communications avec l'ensemble des acteurs du domaine concerné, activant non pas la décision de les adopter, mais la connaissance des pratiques adaptées pour leur mise en œuvre. En ce sens, il ne s'agit plus de pressions normatives ou coercitives mais de pressions mimétiques.

L'isomorphisme mimétique est défini par l'imitation des pratiques d'une autre organisation, conduite par l'absence de connaissance pour une activité incertaine (Lesca et al. 2015). Selon cette définition, les verbatims pour la décision de couvrir les risques n'émergent pas complétement de notre terrain. En revanche, les mesures de sécurité adoptées sont pour partie issues de **pratiques de sécurité traitées par des proches**. Ainsi les comportements **mimétiques identifiés relèvent de celles d'un** père (*« Je prends l'exemple de mon papa qui faisait des sauvegardes fréquentes de ses photos »*) ou d'**un prédécesseur dans la fonction** (*« Mon prédécesseur faisait déjà très attention »*).

Notons qu'un des dirigeants, au début de son activité, assure avoir mis en œuvre une mesure de sécurité parce que les « autres » la pratiquaient, précisément *« …je ne savais pas à quoi cela servait, mais pour avoir un antivirus comme tout le monde … »*. Ce commentaire est cohérent avec les constats de Dlamini et al. (2009 p. 2) précisant que les organisations mettraient en œuvre la SSI « simplement parce que toutes les autres le font ».

[75] L'usage Internet du « monsieur » est justement ce que la réglementation demande de surveiller

Un autre dirigeant précise qu'il avait connaissance de certaines organisations qui ont mis des mesures de protection spécifiques *« pour protéger leurs données nominatives et parce que la loi l'exigeait et d'autres parce qu'ils ont eu un vrai problème ! ».* Ce verbatim appelle plusieurs commentaires quant à l'adoption de pratique par les organisations observées par ce dirigeant et provoquant un effet mimétique. Premièrement, il s'agit d'une mesure de sécurité spécifiquement centrée sur la protection de données. Ensuite, cette mesure de sécurité est exigée par la réglementation (données nominatives). Enfin, il précise que d'autres l'ont mise en œuvre car ils *« ont eu de vrai problème »,* ce qui ne permet pas de définir si ces organisations-là respectaient la réglementation lorsqu'elles ont été confrontées à ce *« problème »*. En ce sens, nous renouvelons notre accord avec la perspective de Williams et al. (2009) qui précisent une combinaison des influences coercitives, normatives et mimétiques, difficiles à isoler, malgré un périmètre d'étude délimité et contextualisé.

Nos verbatims ne font pas émerger d'échanges particuliers d'informations entre les organisations, qu'elles soient concurrentes, fournisseurs (excepté les prestataires informatiques) ou encore clientes. En ce sens, un verbatim illustre la méconnaissance des pratiques des autres organisations : *« Je ne connais pas de concurrents, je vis tout seul dans mon coin non mais c'est vrai je ne connais pas les concurrents, aucune idée de mes fournisseurs je vis tout seul sur mon île… ».* Ces **faibles échanges d'informations** s'inscrivent, en regard de la littérature, dans le principe même de confidentialité de la SSI. D'une part, la SSI n'est réputée efficace que lorsqu'aucun incident impactant ne survient, limitant alors les « histoires à succès » qui seraient alors communiquées ou tout du moins communicables comme une réussite (Hu et al. 2007 ; Kwon et al. 2012). D'autre part, la SSI est un sujet sensible pour lequel les chercheurs de la discipline soulignent la difficulté d'accès à l'information (cf. Kotulic et Clark 2004 et tel que nous en avons fait l'expérience pour notre propre terrain, marquant la réticence de certains dirigeants à évoquer avec nous la SSI et les risques). Si nous portons ces commentaires « opérationnels » au niveau d'abstraction des théories que nous avons mobilisées, nous pouvons porter **un éclairage nouveau sur les difficultés à commenter et partager les risques ou la SSI**. En effet, selon nous, le concept même du risque, d'une part présenté dans le champ de la SSI et d'autre part dans le champ psychologique, n'est **pas communicable « simplement »**. Ainsi, si on en réfère à la littérature, le risque SI se définit comme la combinaison d'une **menace**, d'une **probabilité** et d'une **perte** (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Dhillon et Torkzadeh 2006 ; Sjöberg et al. 2004). Dans le champ de la SSI, l'importance des SI et leur rôle pour les processus d'affaires de l'organisation appellent désormais à considérer cette

combinaison sous l'angle stratégique (Kwon et al. 2012 ; McFadzean et al. 2007 ; Solms et Solms 2005). Ce constat peut conduire à forger des risques spécifiques selon des caractéristiques propres à l'organisation telles que par exemple le mode de gouvernance, la stratégie, le secteur d'activité, ou encore les règlementations. Dans le champ psychologique, nous avons explicité la subjectivité du risque qui définit justement le risque comme un construit social. Rappelons que l'expression d'un risque est individuelle et nécessite de considérer la situation (l'évaluation dans les conditions et l'environnement…) et le contexte (informations propres à l'organisation de l'évaluateur telles que les compétences pour le risque, les processus pour les maitriser…)[76].

Concernant le constat précédent, **nos résultats ne sont pas convergeant avec les conclusions** de Straub et Welke (1998) sur la perception des risques des top-managers. En effet, ces auteurs suggèrent que les croyances de l'exposition au risque de l'organisation des managers s'appuient sur leurs actions SSI entreprises au sein de leur organisation, leurs caractéristiques individuelles et la connaissance des risques qui s'imposent à la même activité et donc aux organisations homologues. Nos verbatims montrent **que les dirigeants interviewés n'ont que peu ou pas de connaissance des risques et des pratiques de sécurité** des organisations comparables à la leur. Ceci peut se justifier par l'uniformité du terrain étudié par Straub et Welke. En effet, ils précisent avoir analysé « deux sociétés classées au Fortune 500 » avec un design de recherche qui nécessitait que les deux entreprises soient « suffisamment semblables » « pour faire des comparaisons significatives »[77] (Straub et Welke 1998 p. 447). Ainsi, le constat de Straub et Welke (1998) **peut s'inscrire dans une approche isomorphique normative de la SSI**, pour laquelle les managers auraient des pratiques de sécurité comparables par la standardisation des cursus éducatifs, ou l'appartenance à des communautés professionnelles (Rizza 2008). Pour les risques SI, cela nous apparait moins pertinent de conclure que les managers d'organisations comparables puissent avoir la même connaissance de leurs risques respectifs. En effet, dans les champs de la SSI et de la psychologie, il y a consensus sur la **spécificité d'un risque** qui est subjectif, situationnel et contextuel[78] (Slovic et al. 1982), et pour lequel la réalité même d'un risque décrit **n'est que partiellement partagée** entre expert et profane (Yates et Stone 1992).

[76] Cf 3.2.8 « Synthèse du chapitre sur la perception des risques » p. 186

[77] Straub et Welke (1998 p. 447) précisent "Customer Processing Company (CPC) was similar to Customer Data, Inc. (CDI) in enough respects to make comparisons meaningful."

[78] Cf 3.2.8 « Synthèse du chapitre sur la perception des risques » p. 186

6.1.7. Conclusion des influences sur la perception du risque SI

Dans les sections précédentes, nous avons **présenté les verbatims caractérisant le risque** qui convergent avec les menaces, les conséquences redoutées et les besoins de sécurité identifiés dans la littérature. L'objet de notre recherche n'est pas, comme l'ont fait Fischoff et al. (1978, 1981) ou Slovic et al. (1979, 1982, 1987) de lister les « déterminants du risque » afin de savoir lesquels interviennent majoritairement dans l'acceptation des situations risquées. Dans une perspective de gestion du risque SI, notre projet vise plutôt à préciser les influences sur la décision d'adopter symboliquement la SSI. De fait, les influences que nous avons identifiées **relèvent davantage de l'importance des SI, de la perception des risques et de l'importance de la SSI**.

Le **SI est caractérisé** comme *« fondamental »* et « très central » dont l'« apport organisationnel » est incontestable et dont les entreprise ne pourraient plus *« se passer »*. Ces constats sont en accord avec ceux de différents auteurs qui soulignent la dépendance appuyée des organisations envers leur SI (Backhouse et Dhillon 1996 ; Bandyopadhyay et al. 1999 ; Ma et al. 2008 ; Peppard et Ward 2004 ; Solms et Solms 2005). L'importance considérée du SI est définie comme une influence majeure dans l'implication des dirigeants et l'adoption de la SSI (McFadzean et al. 2007 ; Siponen 2000 ; Soomro et al. 2016 ; Solms et Solms 2006b ; Straub 1990 ; Wood 1995).

Les risques SI perçus sont également unanimement évoqués par les dirigeants dès lors que l'on aborde la SSI, confirmant alors que la SSI est une discipline de gestion des risques SI (Choobineh et Dhillon 2007 ; Hu et al. 2007 ; Kayworth et Whitten 2010 ; Straub et Welke 1998). Ainsi ces risques sont des évènements vécus ou potentiels, traduisant un impact pour le SI et pour l'organisation. Le concept de risque fait interagir **menaces**, **conséquences** et **probabilités** de survenance (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Dhillon et Torkzadeh 2006 ; Sjöberg et al. 2004). Si les menaces sont très largement décrites, les risques ne traduisent pas toujours la conséquence **et rarement la probabilité de survenance**.

Les menaces ou les sources de menaces évoquées sont concordantes avec celles présentées dans la littérature telles des origines naturelles ou humaines (Loch et al. 1992). Seule la menace interne, elle aussi mentionnée par Loch et al. (1992), semble être peu considérée. Précisément, elle semble effacée par la crainte des menaces externes, ce qui conduite alors à écarter les risques internes. Ces constats trouvent des justifications dans la littérature concernant la SSI et la psychologie du risque. D'une part, Barlette et Fomin (2010 p. 128)

soulignent que les top-managers accordent davantage d'importance aux hackers ou aux virus (risques externes) qu'à l'abus d'initié ou l'erreur humaine (risques internes). En ce sens, Taylor (2006 p. 1582) évoque une vision subjective et étroite des risques conduisant à une perception erronée (autrement nommée « cécité » des top-managers). D'autre part, nous pouvons mettre en perspective cette faible considération pour le risque interne en regard de plusieurs constats sur la perception du risque et qui convergent vers la notion de « contrôle ». La notion de contrôle de la situation est partagée par plusieurs auteurs et conduit les évaluateurs à accepter les risques car ils pensent les maitriser. En effet, Slovic (1982a) soutient que la « maîtrise » du risque relève de la capacité perçue par l'évaluateur à contrôler les dommages qu'il occasionnerait. Les activités pour lesquelles les top-managers s'engageraient « volontairement » (tel que le management de leur collaborateur) faciliterait leur acceptation d'un risque qu'ils pensent alors contrôler[79]. À l'inverse, des menaces sur lesquelles ils ne peuvent agir telles les menaces externes non volontaires[80] comme l'inondation ou l'incendie ou les menaces externes volontaires[77] comme les virus ou les hackers, **accentueraient la perception d'un risque plus important car subi** (Sjöberg et al. 2004 ; Slovic et al. 1984 ; Starr 1969). Nos verbatims montrent l'exemple de plusieurs dirigeants qui ont subi ou évité de justesse les conséquences d'un risque dont la source de menace était « interne ». Bien qu'ils aient été confrontés à ces conséquences, ils n'ont pas entrepris de couvrir ces risques pour qu'ils ne surviennent pas à nouveau. Kermisch (2010) évoque en ce sens un optimisme irréaliste d'individus qui pensent contrôler le risque, développé par la volonté de **réduire l'anxiété inhérente** et les conduisant ne pas considérer la menace. Les travaux de Huang et al. (2010), basés sur le cadre théorique du paradigme psychométrique, font émerger six facteurs pouvant influencer la perception de la SSI. Bien que la contrôlabilité soit évoquée comme facteur et définie comme la possibilité de contenir les menaces, Huang et al. (2010) ne le retiennent pas comme influence majeure[81]. Selon nous, en regard de nos résultats, la notion de contrôle du risque (ou de maitrise) est majeure dans la perception de l'exposition au risque, pouvant ainsi limiter la considération des décideurs pour **la probabilité de survenance des risques**.

[79] Les résultats de Loch et al. (1992) donnent une perspective à une incohérence qu'ils relèvent dans leurs résultats entre perception élevée des menaces et faibles perception de sa probabilité (cf. « 3.2.7 Loch et al. (1992), Réalité des menaces d'aujourd'hui, compréhension d'hier p. 167)

[80] Au sens de Loch et al. (1992))

[81] Nous avons détaillé leur design de recherche, qui, selon nous, biaise le concept de risque et peut alors éclairer les raisons de ne pas retenir ce facteur (cf. « 3.2.7 » Huang et al. (2010), perception de sécurité de l'information p. 182)

En effet, nous avons démontré spécifiquement pour le risques SI, et en accord avec les constats de la littérature de psychologie, que les conséquences sont davantage considérées, **au détriment des probabilités**. D'une part, la difficulté d'évaluer la probabilité d'un risque est soulignée (Slovic et al. 1979) renforçant l'incertitude, caractéristique fondamentale de l'évaluation d'un risque. D'autre part, cette incertitude accentue la rationalité limitée des évaluateurs, qui ne sont pas toujours en capacité de définir des catégories de perte possible (cf. « Jane Smith », Yates et Stones 1992) ne permettant pas de concevoir une conséquence qu'ils n'ont pas déjà vue (Fischhoff et al. 1978 ; Slovic et al. 1980). En ce sens, plusieurs auteurs soulignent la conception constructiviste du risque (Cadet et Kouabénan 2005 ; Kermisch 2012 ; Slovic et al. 1987 ; Sjöberg et al. 2004 ; Tansey et O'riordan 1999), précisant l'influence socioculturelle, la subjectivité, la dépendance au contexte et les caractéristiques idiosyncratiques de l'individu, dont l'appétence au risque (Wildavsky et Dake 1990). Particulièrement, la dépendance au contexte nécessite, dans nos travaux, de considérer une construction du risque enrichie des spécificités de l'organisation telles que, par exemple, le mode de gouvernance, la stratégie, le secteur d'activité, ou encore les règlementations. En ce sens, nous avons montré que, **contrairement aux conclusions de Straub et Welke (1998),** la connaissance des risques des autres organisations n'est pas nécessairement acquise. L'absence de connaissance des risques d'une activité comparable à celle de l'évaluateur ne peut alors nourrir sa réflexion pour l'évaluation du risque.

L'importance de la SSI est signifiée dans les propos des dirigeants, en regard des risques perçus, des menaces et des conséquences. En ce sens, l'acceptation des risques des dirigeants n'est pas acquise sans que soit définies des mesures de sécurité. De plus, certains dirigeants, malgré des mesures couvrant potentiellement les risques qu'ils redoutent, souhaitent contrôler et tester leur sécurité. Ainsi, la SSI est qualifiée d'importante pour plusieurs raisons. Premièrement elle est mentionnée en regard du **rôle stratégique du SI** dont les dirigeants et les organisations ne pourraient se passer. Deuxièmement, les **menaces** sont au moins partiellement connues et les dirigeants semblent enclins à les contrer avec des mesures de sécurité. Troisièmement, les **exigences réglementaires** appuient la nécessité de disposer d'un SI qui ne soit pas affecté par des conséquences qui remettraient en cause le fonctionnement ou les données de l'organisation. Enfin, la SSI est mise en perspective des **conséquences redoutées** que nous avons **prolongées par la désorganisation et la perte de temps**, manifestement redoutées par les dirigeants.

6.2. Les influences sur la décision d'AS

Dans cette seconde partie, nous discutons des influences identifiées précédemment sur la l'adoption symbolique de la SSI. Précisément, il s'agit de comprendre comment, lors des différentes phases de la décision d'adopter symboliquement la SSI, elles sont mises en interaction et prises en comptes pour la perception des besoins, le renseignement sur la solution et son évaluation. En d'autres termes, comment elles sont susceptibles d'amener un dirigeant à la conclusion que la SSI est pertinente pour son organisation.

6.2.1. Perception des besoins

La perception du besoin repose sur la volonté de répondre à des risques potentiels et / ou d'observer la SSI en tant que concept. En effet, rappelons que Straub (1990) mentionne que la préoccupation pour la SSI des managers est fonction du niveau de risque perçu et que la littérature souligne l'analyse de risque comme première étape du processus de l'adoption de la SSI (Wood 1995). Ainsi, nous observons, dans le même temps, l'importance accordée au SI et la mise en perspective des risques et surtout de leurs conséquences

Nous avons détaillé l'importance accordée par les dirigeants à leur SI dans la section précédente. D'une part, cette influence sur la perception du besoin nous semble prégnante en regard du consensus de la littérature sur la **dépendance entre activités de l'organisation et le SI** (Bandyopadhyay et al. 1999 ; Goodhue et Straub 1991 ; Solms et Solms 2006a). D'autre part, la responsabilité des dirigeants est engagée pour protéger ses SI, soit la « bonne gouvernance » visant « le succès de l'organisation » (Solms 2001b ; McFadzean et al. 2007 ; Moulton et Coles 2003 ; Straub et Welke 1998) signifiant alors qu'ils doivent répondre à de potentiels dysfonctionnements, soit **les conséquences d'un risque**. Gerber et Solms (2005) confirment l'importance accordée à la SSI en regard de la contribution des SI à l'activité de l'organisation. Précisément, McFadzean et al. (2007) soutiennent que les entreprises dont le SI est utilisé comme « une arme compétitive dans un environnement à haut risque » investiront davantage dans sa protection. L'intérêt porté au besoin de protéger le SI peut aussi être mis en perspective de la recherche en psychologie qui souligne que plus une activité est perçue comme risquée plus l'évaluateur investira les mesures de sécurité pouvant **rendre le risque acceptable** (Cadet et Kouabénan 2005 ; Slovic et al. 1979).

Ainsi, nous relevons dans les verbatims une prise de conscience[82] pour les risques potentiels pouvant constituer le concept de « bonne idée » d'adopter symboliquement la SSI. **Ces prises de conscience, issues de risques souvent vécus, parfois imaginés**, se déclinent au travers des conséquences possibles et sur les menaces redoutées. Par exemple, un dirigeant qui s'estimait à l'abri des risques SI pour plusieurs raisons a révisé sa réflexion lorsqu'une contamination virale a bloqué tout son SI. En effet, se qualifiant de non paranoïaque, avec un chiffre d'affaires réduit, le besoin de protéger ses SI ne lui apparaissait pas, malgré les préconisations de son prestataire et de ses amis. Après avoir essuyé les conséquences de deux problèmes successifs, la SSI lui semble devoir être observée comme une solution possible (*Ça a pris de l'importance quand il y a un an on a pris un virus ransomware et là on s'est dit ''oh, alors là c'est la m…, vraiment ! À partir de là j'ai pris des décisions pour sécuriser notre système…).*

Avec des conséquences moins engageantes mais vécues, deux autres dirigeants ont eu une perception différente des risques SI, **dès lors qu'ils y ont été confrontés**. Ainsi, pour le premier, c'est l'idée qu'il pouvait perdre ses données et du temps pour les recouvrir qui l'a convaincu de s'engager dans une réflexion pour les protéger (« *Ce dont on* ***a pris conscience à*** *ce moment-là c'est l'importance de ces données, quand on s'est rendu compte… que si on venait à perdre des jours des jours des jours comme ça … ce serait des milliers d'heures de perdues »).* Le deuxième dirigeant évoque, après avoir compris qu'il ne pouvait *« se permettre de laisser passer des données à l'extérieur ou n'importe où sur Internet »* a décidé d'engager des mesures pour protéger ces données (*« Et donc quand j'ai pris conscience de ça, je me suis dit qu'il fallait* ***protéger nos informations des risques*** *qui pouvaient nous tomber dessus.* ***J'ai pris plusieurs décisions sur le matériel, la protection des données…) ».***

Pour un quatrième dirigeant, déjà engagé pour la SSI mais n'ayant pas couvert un risque qu'il savait possible, **c'est la survenance de ce risque dont le menace était interne qui a provoqué un changement de pratique**. Précisément, pourtant averti de l'importance majeure des menaces internes à l'entreprise en regard des menaces externes et dont il avait été informé, un de ses ingénieurs informatique a exposé le SI de l'organisation en adoptant volontairement des mauvaises pratiques (*« …du jour au lendemain c'est devenu une catastrophe ! Bon on s'en est séparé mais n'empêche que là j'ai vu tout le risque et là on a vraiment perdu du temps pour tout remettre d'équerre et donc là ça a été vraiment pour* ***moi***

[82] Les verbatims précisant ces « prises de conscience » sont indiqués dans la section « 5.2.5 Synthèse des risques perçus, des menaces et des conséquences » p. 271

une prise de conscience *on m'en avait déjà parlé qu'aujourd'hui le risque est quand même finalement est beaucoup plus important en interne qu'en externe. »)*.

Nous rapprochons ce constat des commentaires de plusieurs auteurs indiquant une aversion plus marquée pour les risques dont la menace est moins interne qu'externe[83] (Barlette et Fomin 2010; Kankanhalli et al. 2003 ; Loch et al.1992 ; Slovic et al. 1982 ; Taylor 2006). En ce sens, rappelons que Kermisch (2010) fait l'hypothèse d'une volonté de réduire l'anxiété inhérente par un optimisme irréaliste. Ce constat est basé sur l'idée d'un contrôle accru du risque issu de l'interne, sur lequel l'évaluateur disposerait d'un volume d'information important, ce qui est sans doute moins avéré pour les risques externes. Selon ce point de vue, l'hypothèse de Kermisch (2010) s'inscrit alors dans les propos de Cadet et Kouabenan (2005 p. 11) pour qui les évaluateurs font « des pronostics en présence d'incertitude à partir des informations présentes ». Ces constats mis en perspectives de nos verbatims accentuent encore la proximité des concepts entre évaluation des risques dans le champ psychologique et dans le champ de la SSI.

Nous pouvons aussi rapprocher ces constats d'une volonté de rechercher la cohérence dans les évaluations par les individus. En effet, rappelons le rôle de l'affect, mis en exergue par Alhakami et Slovic (1994) ou, encore, Finucane et al. (2000). En particulier, ces auteurs soulignent qu'une activité est considérée moins risquée dès lors que les bénéfices sont perçus comme élevés. En perspective de la fonction des SI, dans les organisations dont nous avons interviewé les dirigeants, il s'agit alors d'opposer conceptuellement les apports des SI en regard des risques qui l'exposent. Autrement dit, leur apport peut apparaitre suffisamment important aux yeux des dirigeants pour que leur perception des risques en soit diminuée.

Toutefois, dans le détail de cette prise de conscience pour le risque SI, les conséquences redoutées éclairent l'aversion au risque SI des dirigeants. Ainsi, nous avons détaillé et explicité les conséquences objectivée par les dirigeants. Si ces conséquences sont parfois évoquées en termes techniques tels que la perte de confidentialité ou de disponibilité, dès lors qu'elles sont repositionnées dans le contexte global des risques pour l'organisation, nous pouvons **les mettre en perspective des impacts pour le dirigeant, l'entreprise et ses métiers** (cf. Les conséquences directes sur l'entreprise et sur le dirigeant p. 321 et Les conséquences « métier » p. 323).

[83] En détail, rappelons que si les résultats de Loch et al. (1992) soulignent une crainte importante des menaces extérieures à l'organisation, alors que près de la moitié des risques relèvent d'acteurs internes (sur 71,8% des réponses 11,7 % pour les menaces externes et 60,1% pour les menaces internes).

Ainsi, selon le paradigme psychométrique du risque, la décision de traiter les risques relèvent, non pas du risque lui-même, mais semble « plus fortement liée à la sévérité des conséquences » (Sjöberg et al. 2004 p. 20). Précisément, cette décision relève des caractéristiques de conséquences qui seraient « immédiates », sévères, qui ne seraient pas parfaitement connues, qui s'inscriraient dans le temps et qui seraient « irréversibles » (Kermisch 2010 p. 50 ; Sjöberg et al. 2004 ; Starr 1969).

Enfin, nous notons que la deuxième formulation du risque, précisée uniquement dans le champ de la SSI, n'est pas évoquée. En effet, si les risques, les menaces, les conséquences et, de façon plus voilée, les probabilités, les vulnérabilités (Willison et Backhouse 2006) ne sont abordées qu'à la marge, par un des dirigeants. Celui-ci a décrit une vulnérabilité d'un protocole de télécommunication (Session Initiation Protocol, SIP), qui, attaqué par « nos amis israéliens et russes » leur permet de *« prendre le contrôle d'un compte »* pour *« revendre les minutes communications que ce soit par le satellite ou par des pays où c'est assez cher »* avec pour conséquences *« une note que vous allez devoir régler et qui peut être de 200 ou 300 000 € en une nuit, c'est énorme ! ».* Outre cet échange qui a permis d'allier vulnérabilité d'un protocole et conséquences financières importantes, les vulnérabilités ne sont pas mentionnées.

Cependant, **les vulnérabilités** sont prises en compte dans différents travaux, selon une approche technique (Baskerville 1993 ; Kotulic et Clark 2004), une approche d'analyse de risque ou encore selon une approche de l'évaluation du niveau de risque en regard des « vulnérabilités / menaces » (Albrechtsen et Hovden 2009 p. 485). Par exemple, Whitman et Mattord (2009 p. 118) précisent l'importance de considérer « l'identification des vulnérabilités dans le SI d'une organisation […] pour assurer la confidentialité, l'intégrité et la disponibilité de tous les composants du SI ». Selon nous, l'étude des **vulnérabilités** du SI permettrait d'en **estimer le niveau d'exposition au risque**. Cette étude, en complément d'une analyse de risque au sens de Choobineh et Dhillon (2007) ou encore de l'ISO/CEI 27005 (2011), permettrait d'objectiver la faillibilité du SI ou, en d'autre termes, l'exposition au risque. Une fois notée cette perspective méthodologique, il est nécessaire de préciser qu'elle ne pourrait survenir avant que le dirigeant initie une analyse de risque SI, soit avant qu'il ne perçoive le besoin de la SSI… En ce sens, dans cette phase de l'adoption symbolique, nous **ne constatons pas une considération exacerbée pour les vulnérabilités des actifs** technologiques telle que le soulignent plusieurs auteurs (Albrechtsen et Hovden 2009 ; Dhillon et Backhouse 2001 ; Doherty et al. 2001 ; Spears et Barki 2010). Nous faisons alors l'hypothèse que **l'accent est mis sur les aspects technologiques** dès lors qu'il s'agit de

mettre en place des mesures de sécurité, soit dans la phase B de Klonglan et Coward (1970), après l'adoption symbolique de la SSI.

Indépendamment d'une faible perception de l'exposition au risque et des vulnérabilités, les dirigeants interviewés **n'ont pas accepté le risque SI « brut »**, à savoir sans aucune mesure de sécurité. L'acceptation du risque, en regard des travaux pour le paradigme psychométrique et des constats établis dans le champ de la SSI, se définit comme une valeur intermédiaire de référence entre avantages et conséquences négatives (Fischoff et al. 1981). Précisément, l'acceptabilité repose sur plusieurs éléments, notamment développés par Slovic et al. (1979, 1982, 1987), tels que par exemple les connaissances scientifiques, la législation, les expériences, la responsabilité vis-à-vis du risque, la profession exercée et aussi, selon Cadet et Kouabénan (2005), les mesures de **sécurité préventives effectives**. En ce sens, notons qu'un des dirigeants (D12), s'il semble accepter les risques SI, ou, tout du moins ne pas s'en soucier, adosse son SI à un hébergeur spécialisé dont il vante la compétence en SSI, et s'appuie également sur un ingénieur informatique interne pour les réponses techniques à sécurité de l'information.

Ainsi, ces constats permettent d'éclairer l'importance perçue des risques SI dans la décision de s'intéresser à la SSI. En effet, selon l'importance du SI et de la SSI et la notion de responsabilité constaté dans nos verbatims, tant sur les plans financiers, image ou juridique, les dirigeants sont, ou seraient, directement impactés par la survenance d'un risque. Outre les conséquences pour le fonctionnement des activités de l'entreprise, les conséquences les atteignent directement, d'une part en tant que responsable de ces organisation et d'autre part car ils seraient obligés de gérer les impacts défavorables que le SI et leurs activités subiraient. En regard du modèle d'adoption symbolique de Klonglan et Coward (1970), la prise de conscience semble parfaitement s'adapter à l''étape de **« conscience »** de la phase de reconnaissance d'un **besoin** notamment développée par (Lesca et al. 2015). Précisément, il s'agit d'une étape dans laquelle **le besoin est identifié** qui est traduit par la prise de conscience d'un **risque à évaluer**, soit la perception des risques ou la solution innovante elle-même, soit la SSI (Rogers 2003 ; Sapp et Korsching 2004).

6.2.2. Renseignement sur la solution

Ainsi, les besoins énoncés sont définis principalement pour éviter les conséquences redoutées, c'est-à-dire la perte de données, l'indisponibilité du service adossé au SI ou, encore, la perte de confidentialité. Ces exigences de sécurité sont en accord avec les propos

de plusieurs auteurs (Bishop 2003 ; Dhillon et Torkzadeh 2006 ; Whitman et Mattord 2009), sans que l'intégrité ait été énoncée. Dans nos résultats, les renseignements sur les solutions possibles aux risques identifiés, reposent sur des **connaissances personnelles,** des connaissances partagées par des **réseaux d'influence,** et enfin, **des connaissances acquises auprès de prestataires**

Ainsi, les connaissances personnelles sont mentionnées telles des **pratiques personnelles** (« *le coté informatique m'intéresse à titre personnel donc je ne suis pas démuni* » ou *« parler avec des gens, voir comment ils fonctionnent et peut-être aussi à l'armée où j'ai appris des façons de de faire.* »). Ces connaissances peuvent aussi provenir de pratiques professionnelles apprises dans des **fonctions occupées antérieurement** *(« En fait, j'étais inspecteur chargé de contrôler, de former de diriger les courtiers, donc je connaissais ça au quotidien de mettre en garde […] sur le plan des données… »* ou *« … j'étais dans la partie informatique »).*
Ensuite**, les réseaux d'influence** représentent une source d'information identifiée et activée par les dirigeants. Tout d'abord, les dirigeants semblent échanger avec leurs amis sur ces problématiques de risques ou plus particulièrement de SSI (*« Alors, j'ai eu un **copain** qui a 3 ou 4 sociétés je crois et qui m'a dit ''moi je me suis libéré de tout ça. […] je gère tout de là et j'ai viré toutes les sociétés informatiques …''. »* ou *« Je ne sais pas : c'est la TV, c'est un **ami** spécialiste en sécurité, c'est le bon sens… »* ou encore *« J'ai aussi **plusieurs amis** qui m'ont donné pas mal d'informations et de contacts pour mettre en place des procédures de sécurité »).*
Aussi, la fréquentation de clubs professionnels voire de particuliers qui sont informés, peut alimenter la connaissance sur les solutions de sécurité possibles (« *Il y a plein de **clubs** … »* ou *« …j'ai des **particuliers et des professionnels** dans mon entourage […] je me dis que **l'expérience de quelqu'un va me servir à moi** […] et **on peut voir si on peut mettre ça ou ça en place**. »* ou encore *« Oui, quand on se rencontre au syndicat, on discute. Eux nous font remonter des informations, des alertes »* et enfin *« quand on se rencontre **au syndicat**, on discute. Eux nous font remonter des informations, des alertes... […] un ensemble d'outils grâce auquel on peut lire, voir ce qu'on avoir, ce qu'on échange. »).*

Enfin, les **prestataires « informatique »** sont également une source d'information (« *je suis conseillé par un **prestataire** depuis qu'on a installé un ERP »* ou *« … On a fait ça avec **mon informaticienne qui me disait ça c'est bien ou ça ça suffit** par rapport à ta capacité, par rapport à ce que tu as… »* ou encore *« On se renseigne auprès des clients, des fournisseurs, des amis aussi. On va voir **une société de services et on se décide pour quelque chose** »).*

Si nos résultats permettent d'identifier les sources d'informations activées par les dirigeants lorsqu'il s'agit de s'informer sur une solution possible, ils ne permettent pas de statuer précisément sur la nature des informations échangées sur les solutions aux risques. Cependant, les résultats font clairement émerger des besoins centrés sur la disponibilité et, dans une moindre mesure, la confidentialité. Si ces exigences n'appellent pas les mêmes mesures de sécurité, nous avons constaté que les **sauvegardes sont majoritairement évoquées en regard de pertes de données particulièrement redoutées,** répondant alors à la seule exigence de disponibilité des services et des données. Nous pouvons alors faire l'hypothèse de solutions uniformes portées par des professionnels, alimentant alors un isomorphisme normatif et mimétique. En effet, rappelons qu'en situation **d'incertitude**, la recherche de la solution optimale revient souvent à adopter la première solution connue (*satisficing*) telle que développé par March et Simon en (1958) et soulignée par Albrechtsen (2007) pour les options de traitement des risques SI.

Dans ce prolongement, nous avons évoqué **le rôle des prestataires** et les **mesures pratiques** qu'ils peuvent recommander. Dans les deux cas, il est notable que leur préconisations et pratiques proposées ou mises en œuvre peuvent renseigner le dirigeant sur son besoin de couvrir les risques. Cela étant, les dirigeants **nourrissent une critique fournie à l'endroit des prestataires.** En effet, d'une part il apparait que leur conseil semble insuffisant et centré sur l'aspect technique uniquement : *« Je pense que oui. Suffisamment, je ne sais pas mais je pense que oui.* ***Peut-être pas suffisamment, peut-être pas de manière trop négative mais oui****, encore une fois, que ce soit sur la partie antivirus avant, sécurisation, sur la partie craquage d'un Wifi, craquage des données, les ransomware…).* Notons le commentaire d'un dirigeant qui souligne son manque de confiance pour les prestataires : *« le* ***gros défaut des prestataires c'est qu'il se gargarise*** *de leur science donc en fait il vous explique pas trop… je veux dire ils vous baratinent, ils vous expliquent pas bien les choses et puis c'est double tranchant parce qu'on va rencontrer quelqu'un qui va prendre le temps de vous expliquer calmement les choses et on va se dire* ***il est en train de vendre son truc****… ».* D'autre part, donnant son avis sur des risques, selon, là aussi une vision technique de la SSI, l'informaticienne d'un des dirigeants explique ce qu'il est nécessaire de mettre en œuvre ou pas, conduisant le dirigeant à conclure qu'*« elle a été un petit peu plus dans la minimisation des risques plutôt que de mettre en perspective les potentiels problèmes qu'il pourrait y avoir »*.

Les critiques dépassent la fonction de conseil des prestataires pour remettre en cause leur capacité à gérer les solutions qu'ils ont eux-mêmes proposées. Deux dirigeants découvrent *« par hasard »* que leurs données ne sont plus sauvegardées, « *sans savoir depuis combien de temps ça a duré… »* avec pour conséquence directe pour le second que *« … depuis 6 mois, les*

mails n'étaient pas sauvegardés ». Un autre dirigeant émet de « sérieux doutes » quant aux méthodes et procédures de son prestataire sur la capacité à restaurer les systèmes de ses clients. Enfin, le quatrième dirigeant précise une défaillance de son prestataire, identifiée lorsqu'il a s'agit de restaurer des données *(« La dernière sauvegarde elle avait 3 mois chez eux et quand je vois ça, je leur dis ''mais où sont toutes mes données depuis 3 mois-là ?'' »).* Face à cet incident, le prestataire ne prend pas ses responsabilité (*« Réponse : ''ah oui oui, mais en fait il n'y a pas de sauvegarde'' »* et rejette la faute sur le dirigeant (*« le problème venait justement -comme par hasard- de mon PC qui commençait à avoir des signes de fatigue »*).

Si selon Rogers (2003) les prestataires doivent être vus « par les potentiels adoptants comme n'ayant pas d'intérêt personnel significatif dans l'adoption ou dans le rejet de la nouvelle technologie », **il semble que ce ne soit pas toujours le cas** pour les dirigeants interviewés.

Ces constats renforcent notre propos sur la combinaison des influences normatives et mimétiques sur la gestion des risques, pour lesquels l'incertitude conduit à adopter la première solution connue (Albrechtsen 2007). À nouveau, cette combinaison est parfaitement décrite dans les travaux Williams et al. (2009), qui ont démontré que l'adoption de mesures de sécurité peut être influencée par des pressions normatives internes et externes et des pressions mimétiques. S'agissant des échanges avec les prestataires, Rizza (2008) souligne l'homogénéisation des pratiques qui s'inscrit dans un comportement d'adoption des normes et techniques les plus adéquates du domaine.

Particulièrement au recueil d'informations sur les réponses possibles au risque, Douglas et Wildavsky (1983) indiquent que le partage de **valeurs, des croyances et une culture commune**, peuvent être mis en perspective des styles de pensée qui régissent l'action sociale des individus. En ce sens, rappelons que les valeurs partagées se combinent dans certains contextes sociaux et culturels, les biais culturels, pour former la **perception des risques des individus**. Spécifiquement aux travaux sur l'adoption symbolique, Sapp et Korsching (2004 p. 352) soulignent l'importance « des croyances normatives perçues » pouvant conduire à la décision d'adoption ou de rejet symbolique. Ainsi, ces échanges peuvent conduire à un consensus sur l'adoption d'une pratique qui pourrait ne pas correspondre au besoin spécifique du risque à couvrir.

Les verbatims montrent des pratiques orientées majoritairement sur la sauvegarde, laissant alors penser que le recueil d'information offre une perspective sur des aspects pratiques de la SSI. Cela rejoint renforce le constat dressé dans la section précédente et décrivant des mesures de sécurité centrée sur les **aspects technologiques**. En ce sens Dhillon et

Backhouse (2001 p. 137) indiquent une « tradition fonctionnaliste » de la SSI, ayant tendance à se concentrer **sur les moyens et non sur les fins.** L'articulation de l'étape une (perception des besoins) et deux (recueil d'information) s'oriente vers des mesures pratiques et technologiques, omettant le modèle de gestion des risques décrit dans la littérature et dont la première étape relève de « l'identification et de la formulation de problèmes en ce qui concerne le risque SI » (Straub et Welke 1998 p. 453).

Nous constatons **que le recueil d'information ne porte alors pas complétement sur la SSI mais davantage sur une réponse ponctuelle à un besoin selon une rubrique réduite** (soit la sauvegarde dans nos résultats). Selon nous, le recueil d'information sur la SSI devrait conduire non pas à détailler des mesures techniques mais à s'intéresser aux risques avérés pour l'organisation. En effet, rappelons que l'approche risque pour le SI, combinant menace et probabilité (Bandyopadhyay et al. 1999) permet de **synthétiser les besoins de protection du SI**.

6.2.3. Évaluation de la solution

Dans le modèle d'AS adapté à la SSI, cette étape vise à projeter de façon abstraire la SSI (Karahanna et al. 1999 ; Rawstorne et al. 1998). Cependant, nos résultats sont issus d'organisation dans lesquelles les mesures de protection sont implémentées, parfois depuis plusieurs années, ce qui n'a pas permis, fidèlement à cette phase de l'AS, de recueillir les réflexions des dirigeants. Cela étant, ils se sont prononcés sur l'idée que **la SSI répondait ou pouvait répondre à leur besoin**.

Ainsi, certains dirigeants mettent en perspective les mesures de sécurité déployées en regard des risques qu'ils redoutent. Par exemple, l'un d'entre eux détaille son plan de secours informatique pour le soumettre « virtuellement » à tous les risques imaginés : *« … pour moi, c'est une question de probabilités et de statistiques.* ***Il y a plusieurs couvre-feux****, mon ordinateur que* ***j'essaye d'entretenir*** *dans le sens où* ***j'ai pour habitude tous les deux ou trois ans de changer d'ordinateur*** *et de tomber en panne avec un backup sur un premier disque dur de manière à vraiment* ***disposer d'un miroir*** *pour disposer d'une* ***procédure*** *qui me permet en quelques heures d'aller racheter un ordinateur et retrouver exactement la même configuration, le* ***backup est fait en réalité sur deux disques*** *dur lim****itant alors la perte de données du premier*** *s'il venait à dysfonctionner, lorsque je m'absente plusieurs jours, j'essaye de ne pas* ***les stocker au même endroit*** *pour éviter une problématique de vol ou d'incendie ou de dégât des eaux, je ne sais pas, et puis il y a encore un plan C ou le contenu des données*

importantes tient dans un volume assez réduit permettant de les synchroniser sur des offres cloud … ». À la fin de sa projection, il conclut *« Avec cet ensemble, j'ai la sensation qu'il faudrait vraiment un* ***cataclysme pour que cela ne fonctionne plus****… »*

D'autres dirigeants, tout en étant convaincus qu'il s'agit de bonnes pratiques, réfléchissent à améliorer et/ou éprouver les mécanismes de sécurité existants voire à les prolonger. Ainsi, le premier déclare : *« **Oui, je pense*** (que mes risques sont couverts)*. […]. On pourrait toujours faire plus comme je l'ai dit, oui la sauvegarde à la seconde… […].* ***Pour l'instant je pense que c'est bien. »*****.** Le second est engagé dans un projet de sauvegarde pour renforcer sa sauvegarde : *« On n'****est pas encore protégés jusqu'au bout****, il manque encore un chainon,… la sauvegarde automatique fonctionne bien sur nos PC mais il faudrait avoir une* ***sauvegarde de sauvegarde qui soit hébergée*** *…* ». Le troisième veut mettre à profit une avancée technologique pour parfaire sa sauvegarde*: « Jusqu'alors on n'avait pas la fibre donc maintenant qu'on l'a il faut que je réfléchisse à un système de sauvegarde sur le cloud directement mais je ne l'ai pas encore fait… »*

Un dirigeant n'est pas complétement satisfait de la maitrise de ses risques. Il évoque le manque de compétence sur la mise en œuvre et la volonté de contrôler l'efficacité de ses mesures de sécurité pour laquelle il regrette le manque de compétences (*« … mais je suis convaincue que la fiabilité à 100% n'y est pas dans ma structure, mais comme dans quelle autre structure, parce qu'on n'a pas suffisamment de compétences »* et *« Je* ***pressens forcément un manque de fiabilité****. Je prends ma voiture : elle fonctionne, elle fonctionne, elle fonctionne, jusqu'au jour où j'aimerais qu'on s'arrête, qu'on ouvre le capot et qu'on me dise ça c'est bon, il ne manque pas d'huile, il ne manque pas ça. Il y a ce qu'on a écrit et il y a la capacité à vérifier ce qui a été écrit. Et moi* ***je n'ai pas de compétences en informatique****. ».* Ce manque de compétence peut être mis en perspective des propos de Kankanhalli et al. (2003) pour qui souvent, les tops-managers manquent de connaissances des contres mesures possibles, ce qui corroborerait ces constats. Cependant, la phase précédente devrait permettre justement au décideur d'acquérir les connaissances nécessaires sur les protections possibles (Hagen et al. 2008). En ce sens, pour Straub et Welke (1998) l'implication des directeurs ne peut se faire que dès lors qu'ils sont informés de la gamme complète des mesures disponibles et qu'ils mettent en œuvre les mesures les plus effectives. Ceci est concordant avec les commentaires de plusieurs auteurs qui soulignent que la SSI est observée prioritairement sous la lentille technique (Dhillon et Torkzadeh 2006 ; Posthumus et Solms 2004 ; Taylor 2006), soit un thème de la SSI que les dirigeants n'investissent pas. En ce sens, Peltier (2004) précise qu'en l'absence d'approche cohérente de la SSI, les mesures de sécurité peuvent être

définies « ex nihilo » sans que leur pertinence soit justifiée et qui seraient alors déployées par mimétisme[84]. Nos résultats ne montrent pas d'orientation claire sur la compétence des dirigeants à déterminer leur mesure de sécurité « pratiques », au profit des prestataires qui pourraient alors être prioritaire sur cette décision « technique ». Le commentaire d'un des dirigeants s'inscrit dans cette perspective. Après avoir évoqué son constat sur la faiblesse des sauvegardes des entreprises, il suggère *« **la méconnaissance** »* avant de poursuivre pour préciser que *« si demain on arrive à leur dire écoutez, ne vous inquiétez pas, vous payez… et vos postes sont sauvegardés de façon sécurisée sur le Cloud etc… ça leur va bien »*.

Plusieurs dirigeants soulignent que, bien que ce soit une bonne idée, la déclinaison en mesures de sécurité effectives n'est pas toujours engagée par manque de moyen, de ressource ou de temps *(« C'est comme la cybercriminalité quand vous écoutez les mecs faut tous se prendre pour le GIGN et la NASA réunis pour tout protéger tout oui quand on est chef d'entreprise on **fait ce qu'on peut avec les moyens qu'on a…** »* et *« Cela fait partie des seconds dossiers qui passent après toutes les urgences et **quand on y confrontés**, c'est un peu le principe de l'assurance, quand on doit payer on se dit ah mince je n'étais pas bien protégé, ah mais vous n'étiez pas assuré non plus »*). En complément un dirigeant pense pouvoir disposer des informations de son prestataire, permettant alors d'évaluer la solution, mais souligne le manque de réalisation pratique : *« …il y a des choses dont j'ai entendu parler et qui ont l'avantage de me mettre la conscience dessus. Après, qu'est-ce qu'on en fait réellement, je ne suis pas sûr de mettre en place grand-chose en toute honnêteté. J'y pense mais malheureusement après, **pris dans le quotidien**, je ne suis pas en train de réfléchir moi-même au papier que je suis en train de mettre dans ma poubelle. »*. Ce constat relève plutôt de l'adoption matérielle de la SSI, hors du champ de notre étude mais qui dénote la « dissonance » d'AS (Karahanna et al. 1999 ; Rogers 1995) renvoyant à une décision pour laquelle **l'adoption symbolique est en désaccord avec l'adoption réelle**.

6.2.4. Conclusion des influences sur la décision d'AS

Dans cette seconde partie, nous avons présenté les verbatims concernant la décision d'adopter symboliquement la SSI puis précisé leurs interactions pour les confronter à notre cadre théorique. Le modèle d'adoption symbolique adapté à la SSI se présente comme un processus en trois phases qui peut conduire à l'adoption ou au rejet d'une bonne idée. Nous

[84] Pour dépasser ce biais, Peltier (2004 p. 48) recommande d'effectuer une « **analyse de risqué** » pour assurer que « toutes les décisions sont basées sur les besoins de l'entreprise et que les mesures prudentes et raisonnables sont mises en œuvre »

avons détaillé les trois phases selon la perspective du risque dans le champ psychologique et dans le champ de la SSI.

En regard de l'importance accordée aux SI, il ressort un **intérêt marqué pour les risques**, qui les exposent, source du besoin de SSI, conformément aux remarques de Straub (1990). Précisément, nos résultats font émerger « **une prise de conscience** » qui peut alors engager le dirigeant vers l'étude de la SSI, telle que déclinée dans le processus d'AS. En accord avec la littérature sur le champ psychologique du risque, nos résultats mettent en évidence une faible aversion pour les risques dont les menaces seraient internes (Kankanhalli et al. 2003 ; Loch et al.1992 ; Slovic et al. 1982). Ce constat est renforcé par la notion de contrôle du risque, parfaitement explicitée par Kermisch (2010) qui évoque l'anxiété inhérente à un tel scénario. Comme dans le champ psychologique du risque, les évaluations des dirigeants sont établies principalement sur l'ampleur des conséquences du risques et non sur les probabilités de survenance (Sjöberg et al. 2004 ; Starr 1969).

Les besoins énoncés visent à éviter la perte de données, l'indisponibilité du service ou la perte de confidentialité sur lesquelles les dirigeants se renseignent. Nos résultats montrent que ces **connaissances relèvent** soit **de pratiques personnelles,** soit **de pratiques professionnelles** apprises dans des fonctions occupées antérieurement**,** soit **de réseaux d'influence** et, enfin, **de prestataires** « informatique **».** Pour cette dernière source, nous identifions **un effet mimétique**, les prestataires répondant à la fois à leur client de façon standard par des solutions techniques courantes et **sans les accompagner dans une démarche d'analyse de risque** (Albrechtsen et Hovden 2009 ; Choobineh et Dhillon 2007 ; ISO/CEI 27005 2011). Enfin, nous avons relevé des combinaisons d'influences isomorphiques, telles que le soulignent Williams et al. (2009) ou Kwon et Johnson (2014).

L'évaluation de la solution, qui se définit comme une projection abstraite de la solution étudiée, a permis de mettre en évidence l'acceptation des mesures de sécurité comme étant une bonne idée. En d'autres termes, cela se **traduit dans le modèle d'AS comme justement une adoption symbolique d**e la SSI et non pas un rejet. Ce constat n'est pas partagé par tous les dirigeants, certains visant à revoir leur dispositif pour identifier s'il correspond à leurs besoins « réel », renforçant davantage le recourt **à l'analyse de risque** et rejetant l'empilement de solution techniques isolées.

Plusieurs commentaires peuvent être dressés sur le modèle d'AS adapté à la SSI. Rappelons que Karahanna et al. (1999 p. 185), sur la base des travaux de Rogers (1983), soutient que le

processus de décision d'innovation peut être « conceptualisé comme **un ordre temporel d'étapes** par lesquelles un individu passe de la connaissance initiale, à la formation d'une attitude favorable ou défavorable envers elle, à une décision d'adopter ou le rejeter, de mettre en œuvre l'innovation ».

Premièrement, à la lumière des résultats, il semble que le **modèle d'AS pour la SSI ne se décline pas une unique fois,** mais qu'il soit activé **par le dirigeant dès lors qu'un besoin de sécurité est perçu.** Précisément, chaque risque peut être défini comme un nouveau besoin à couvrir, appelant une étape de renseignement qui offrirait alors une information centrée sur **la protection technique d'un risque**, avant d'être évaluée dans le contexte du décideur. Les verbatims confirment ce constat, tels que par exemple un des dirigeants qui soutient prendre en considérations que les *« petits trucs »* qui *« sont arrivés »* avant de penser à des contre-mesures. Trois autres évoquent **l'adoption dans le temps**, **faite d'itérations** (*« Au niveau de la sécurité je pense que ça se fait au **fur et à mesure** »* et *« comme je disais tout à l'heure, c'est une prise de conscience **progressive**. On progresse, on regarde les autres, on écoute et on finit par s'adapter »* et *« Je ne me suis pas réveillé un matin en me disant qu'il fallait faire quelque chose. **C'est un long cheminement**. C'est des rencontres, des discussions, des expériences malheureuses de confrères ou de clients. »* et enfin *« … des gens peuvent voir nous les voler. Faut aussi faire attention aux virus. Je vous dis ça d'un coup mais nous avons compris **tout ça dans le temps**. »*

Ensuite, c'est davantage une succession d'AS qui conduirait à la SSI au sens de Whitman et Mattord (2009 p. 118), c'est-à-dire « la protection d'informations et ses éléments critiques, y compris les systèmes et le matériel qui utilisent, stockent et transmettent des informations » grâce à « l'identification des vulnérabilités dans le SI d'une organisation […] pour assurer la confidentialité, l'intégrité et la disponibilité des composants du SI ». Ce commentaire est en accord avec la littérature sur l'acceptation du risque. En effet, l'individualité de la décision d'accepter le risque est établie sur des règles complexes combinées à des conséquences multiples dont la connaissance et l'ampleur sont particulières à chaque évaluation (Slovic et al. 1979 ; Yates et Stones 1992). Ainsi, dans la perspective d'une succession d'AS, l'évaluateur ne serait alors plus disposé à étudier un ensemble de risques et décider leur acceptabilité mais à réaliser une évaluation unique pour un risque donné et avec ces conséquences négatives multiples. Ainsi, l'évaluateur centrerait son évaluation sur les conséquences auxquelles il peut accéder en regard des biais de disponibilité (Lichtenstein et al. 1978) et de représentativité (Amalberti 1996), inhérents à toute évaluation du risque.

Cette construction de la SSI renverrait à une approche technique, **à l'opposé des auteurs prônant une vision holistique et organisée** (tels que par exemple Bandyopadhyay et al. 1999 ; Choobineh et Dhillon 2007 ; Dlamini et al. 2009 ; Doherty et Fulford 2006 ; Karyda et al. 2005). Rappelons, d'une part, que cette **vision technique s'inscrit dans une posture réactive des organisations** face aux risques (Doherty et Fullford 2006 ; Kwon et Johnson 2014 ; Vance et al. 2014). D'autre part, elle est décriée pour son **inefficacité à satisfaire les besoins** des organisations, par **l'absence de méthode adaptée** pour analyser les risques (Doherty et Fulford 2006 ; McFadzean et al. 2007) et se limiterait à l'étude des aspects technologiques des SI, **sans considérer les risques pesant sur les activités majeures de l'organisation.**

En synthèse des verbatims représentatifs du processus d'adoption symbolique de la SSI, nous dressons, pour chaque dirigeant, la **nature du besoin en SSI** et les influences sur sa connaissance du risque et de la SSI en **tant que solution**.

	Nature du besoin		**Connaissance de la SSI**		
	Risque[85]	SSI	Le dirigeant lui-même	Son réseau d'influence	La régle-mentation
D1	RV	O	O	O	O
D2	RI / RC		O	O	
D3	RV			O	
D4		O	O		
D5	RI		O		O
D6	RI	O	O	O	
D7		O	O	O	
D8	RI / RC		O	O	
D9		O	O	O	
D10	RI / RV	O	O	O	O
D11		O	O		
D12		O		O	
D13	RI		O	O	
D14	RI / RC		O	O	
D15	RV		O		
D16	RI / RV	O	O	O	O
D17	RC / RV		O	O	

Tableau 19 : Synthèse de la nature et de l'origine des besoins en SSI

[85] RV : sinistre vécu, RI : risque imaginé et RC : risque communiqué. O = le besoin est centré sur la SSI

Chapitre 7. Conclusion générale de la recherche

Une des principales questions à l'origine de notre recherche portait sur la nécessité, pour une organisation, de subir un incident majeur avant de prendre les dispositions adaptées pour assurer la protection de son SI. De fait, dans nos travaux, nous nous sommes attachés à éclairer le processus de décision pour la SSI, en considérant une approche individuelle du risque. À l'appui d'un cadre théorique innovant, nous avons cherché à saisir les influences pouvant intervenir lors du processus de décision de la SSI. Pour ce faire, nous avons mobilisé des théories issues du champ psychologique et du champ institutionnel, complétées par les avancées récentes provenant de la littérature SSI, fédérées dans un cadre théorique l'adoption symbolique. Comme cela a été précisé dans l'introduction générale de ce document, le projet est de faire émerger des éléments de réponse à notre problématique : « Quels sont les éléments considérés et leur influence sur la décision d'adopter symboliquement la SSI ? ».

Autrement dit, nos travaux visent à rendre intelligible les éléments considérés par les dirigeants lorsqu'il s'agit d'adopter symboliquement la SSI et comment ces éléments interagissent et nourrissent leurs réflexions. Notre volonté a été de situer ces influences pour le risque, la SSI et la décision, dans le contexte du décideur pour son organisation, au moment où le cheminement de sa réflexion a été effectué.

Particulièrement, sur la base des modèles des perceptions managériales des risques SI et du modèle de planification pour traiter les risques SI, développés par Straub et Welke (1998), nous avons mobilisé le cadre de l'adoption symbolique de Klonglan et Coward (1970).

Notre intérêt pour cette thématique et cette problématique s'inscrit à la fois dans l'actualité et dans les prolongements théoriques de la recherche d'une discipline réputée « jeune », la SSI. D'une part, de nombreuses enquêtes relèvent l'ampleur et la variété de conséquences liées à la survenance de risques SI, qui selon EMC (2014), impacteraient 4 organisations sur 5. En outre, ces changements sont à mettre en perspective avec l'inflation prodigieuse des incidents et de leurs coûts (Bulgurcu et al. 2010 ; Gordon et Loeb 2002 ; Whitman et Mattord 2016 ; Willison et Warkentin 2013). D'autre part, plusieurs auteurs appellent à étudier les raisons pour lesquelles les top-managers investissent peu, voire pas, la SSI (Barlette et Fomin 2010 ; Kwon et al. 2012 ; Taylor 2006). Précisément, il est demandé de mieux appréhender les éléments sur lesquels les dirigeants fondent leurs perceptions des risques SI (Crossler et al. 2013 ; Dlamini et al. 2009 ; Kankanhalli et al. 2003).

Inscrivant nos travaux dans la perspective d'une dépendance croissante des entreprises envers leur SI (Backhouse et Dhillon 1996 ; Bandyopadhyay et al. 1999 ; CLUSIF 2014) et de l'identification des risques comme point initial de la décision de gérer le risques (Albrechtsen et Hovden 2009 ; Choobineh et Dhillon 2007 ; Kotulik et Clark 2004 ; Mitchell 1995), il apparait donc pertinent de s'intéresser aux influences qui conduisent à l'initialisation du processus de gestion des risques.

Nous proposons dans cette conclusion générale d'exposer les contributions théoriques, méthodologiques et managériales de notre recherche. Nous discuterons également les limites de notre travail. Cela nous permettra, in fine, de proposer différentes voies de recherche afin de dépasser certaines perspectives des résultats présentés dans cette thèse.

7.1. Les contributions théoriques de la recherche

Nos analyses font émerger plusieurs contributions théoriques concernant la compréhension du processus d'adoption symbolique de la SSI.

En premier lieu, nos résultats confirment que la **SSI peut être présentée comme une discipline de gestion du risque** telle que des auteurs spécialisés en SSI l'évoquent (Doherty et Fulford 2006 ; Siponen et Oinas-Kukkonen 2007 ; Solms et al. 1994 ; Wood 1995). Pour cela, nous avons étudié et mobilisé les principaux modèles de gestion des risques SI. Précisément, nous les avons placés en perspective des paradigmes majeurs d'évaluation du risque dans le champ psychologique. Dans les deux disciplines (gestion des risques SI et paradigme psychologique), l'ordre d'enchainement des étapes est comparable et la finalité est commune, à savoir **l'acceptation du risque**. Précisément, il s'agit, pour l'évaluateur, d'identifier, d'estimer les conséquences et la probabilité de survenance du risque, pour décider s'il est acceptable (Fischhoff et al. 1978 ; Slovic et al. 1979, 1982, 1987). Le cas échéant, des **mesures de sécurité doivent être choisies** et mises en œuvre. Nos résultats mettent justement en évidence les risques SI perçus, vécus ou encore partagés que la plupart des dirigeants n'acceptent pas. Selon eux, **ces risques SI ne sont pas acceptables** et évoquent alors des mesures de sécurité pour les couvrir, inscrivant alors la SSI comme **activité de gestion du risque**.

Deuxièmement, la **SSI est présentée comme importante** voire *« fondamentale »* pour les dirigeants, particulièrement en regard du rôle majeur du SI et des conséquences redoutées. Des exigences de disponibilité et, dans une moindre mesure, de confidentialité sont définies

pour l'ensemble des services et données importants du SI. Nos résultats, en accord avec la littérature, soulignent **la dépendance entre le SI, les activités de l'organisation et le besoin de le protéger** (Backhouse et Dhillon 1996 ; Choobineh et Dhillon 2007 ; Kayworth et Whitten 2010 ; Posthumus et Solms 2004 ; Solms 1999). Ainsi, nous mettons en perspective l'intérêt des dirigeants pour la SSI alors que la littérature évoque souvent, tout en le regrettant, une faible implication des top-managers (Barlette et Fomin 2010 ; Doherty et Fulford 2006 ; Goodhue et Straub 1991 ; Hagen et al. 2008 ; Kankanhalli et al. 2003 ; Knapp et al. 2006 ; Kotulic et Clark 2004 ; Kwon et Johnson 2014 ; McFadzean et al. 2007). En ce sens,) puis) appellent à étudier l'investissement des dirigeants pour la SSI. Précisément, nos résultats montrent que **les dirigeants s'intéressent à la protection des SI en fonction des risques redoutés** perçus et exprimés. Nos résultats **confirment l'adoption symbolique de la SSI par les dirigeants**.

Ainsi, l'intérêt des dirigeants pour la SSI se révèle par l'expression des **risques potentiels redoutés.** Ceux-ci sont énoncés tels un danger ou une menace, assortis de conséquences indésirables que le dirigeant a parfois expérimentées mais qu'il souhaite toutefois éviter. Rappelons que le risque est un concept abstrait (Tsohou et al. 2006) dès lors qu'il ne se traduit pas en sinistre (Kermisch 2012) et complexe (Gerber et Solms 2005). Nos résultats montrent que les dirigeants expriment les risques souvent sous le seul angle de la menace. Or, nous savons que la menace[86] seule ne permet pas d'exprimer le risque et qu'il convient d'en indiquer les conséquences possibles afin **d'éclairer l'évaluation du risque** (Cadet et Kouabénan ; Kermisch 2012 ; Yates et Stones 1992). Particulièrement, la SSI se définit comme « un processus continu d'identification et de priorisation du risque de sécurité informatique et la mise en œuvre et le contrôle de mesures qui adressent ces risques » (Spears et Barki 2010 p. 505). Dans cette perspective, nos résultats montrent que, s'il s'agit d'élaborer des réponses adaptées aux problématiques de l'organisation (Soomro et al. 2016), **l'expression du risque ne peut être centrée sur les seules menaces**.

Nos résultats soulignent également la **subjectivité et la contextualité** du risque qui ne se considère pas comme « quelque chose d'extérieur que l'on peut percevoir indépendamment de son contexte » (Kermisch 2012 p. 5). Ces deux caractéristiques du risque peuvent éclairer les **faibles échanges d'informations** identifiés dans nos résultats. Trois points puisés dans la littérature permettent d'expliquer ce résultat. Premièrement, la SSI est un sujet

[86] Pour accéder à une représentation ludique des risques, menace et danger, nous renvoyons le lecteur à l'illustration du « dangereux ours sans risque » développée par Magne (2010, cf. « 3.2.1 » Définition du risque p. 110)

confidentiel sur lequel les organisations souhaitent peu communiquer (Kotulic et Clark 2004). Deuxièmement, Kwon et al. (2012) constatent que les entreprises sont peu enclines à évoquer les dysfonctionnements du SI et les pertes avérées associées. Enfin, attendu qu'une SSI réussie se traduit justement par l'absence de conséquences, Hu et al. (2007) soutiennent que la discipline manque « d'histoire à succès » qui pourraient être échangées. Nos verbatims montrent ainsi que **les dirigeants n'ont que peu ou pas de connaissances des risques** possibles dans les organisations comparables à la leur. Nos résultats nous permettent donc de ne pas confirmer ceux de Straub et Welke (1998) concernant la perception des risques des autres organisations comme source d'influence ou d'implication des dirigeants dans la SSI de leur propre organisation.

Nos résultats révèlent que la **connaissance des responsables des risques et de la SSI** est davantage acquise au travers d'échanges avec les réseaux d'influence, autant les proches que les prestataires, ou les associations professionnelles auxquelles les dirigeants adhèrent ou, encore, par des communications issues des médias. Comme évoqué précédemment, les risques sont surtout **communiqués sous l'angle de la menace**. En effet, les menaces que nous avons identifiées sont parfaitement convergentes avec les travaux princeps de Loch et al. (1992). Précisément, les dirigeants interviewés ont une connaissance étendue des menaces. Il semble donc que **la faiblesse des dispositifs de sécurité ne repose pas sur une méconnaissance des menaces** (comme le suggéraient Willison et Backhouse 2006) **mais davantage sur une vision techno-centrée de la SSI** (Dhillon et Backhouse 2001 ; Karyda et al. 2005 ; Kayworth et Whitten 2010 ; Spears et Barki 2010).

Au-delà des deux conclusions précédentes sur un risque perçu **complexe** et **défini par la menace**, l'analyse des verbatims révèle le peu de considération des décideurs pour les **probabilités de survenance du risque SI**. L'insensibilité à ces probabilités de survenance peut conduire les dirigeants à ne pas considérer les risques. Ce constat est en accord avec de nombreux auteurs en SSI et en psychologie (Cadet et Kouabénan 2005 ; Doherty et Fulford 2006 ; Kermisch 2012 ; McFadzean et al. 2007 ; Slovic et al. 1980). Nos analyses montrent ainsi que les évaluations sont davantage établies sur **l'ampleur des conséquences** et qu'elles **écartent les probabilités** des risques. Elles soulignent également l'**absence de référence sur des risques jusqu'alors non subis**, conduisant les top-managers à **ne pas les considérer**. Ce résultat est convergent avec différentes recherches en SSI (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Taylor 2006). Taylor (2006 p. 1585) évoque ainsi la **« cécité des exécutifs ».** D'autres auteurs parlent de la **posture réactive des organisations face aux risques** (Doherty et Fullford 2006 ; Kwon et Johnson 2014 ; Vance

et al. 2014). Précisément ils indiquent la difficulté d'appréhender les risques lorsqu'il n'est encore « **rien arrivé »** (Kwon et Johnson 2014 p. 452).

Ce résultat remet en cause la définition consensuelle du risque définit par une menace, une probabilité et une perte (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Dhillon et Torkzadeh 2006 ; Sjöberg et al. 2004). En d'autres termes, les risques non traités seraient ceux pour lesquels les dirigeants n'auraient pas suffisamment de connaissances, tant sur les **conséquences que sur leur probabilité**, car, **« écartant de la vue ce qui est en dehors de l'esprit »**, les dirigeants auraient une **perception incorrecte** des événements (Fischhoff et al. 1978 ; Slovic et al. 1980).

Si la probabilité n'est pas évoquée, les conséquences possibles mettent en perspective des besoins de sécurité relatifs à la disponibilité et à la confidentialité. Ces besoins sont étudiés par les dirigeants en recueillant, notamment, des informations auprès de leurs prestataires, qui représentent alors une influence isomorphique normative et mimétique. En effet, nous avons constaté que les sauvegardes sont majoritairement évoquées en regard de pertes de données, particulièrement redoutées, conduisant les professionnels à proposer des solutions uniformes. En effet, rappelons qu'en situation d'incertitude, la recherche d'une solution revient souvent à **adopter la première solution connue** qui serait alors proposée par un prestataire, en accord avec les options de traitement des risques soulignées par Albrechtsen (2007). En ce sens, les prestataires auraient un rôle triple, influenceur sur le risque perçu, influenceur sur le traitement du risque et prescripteur de la solution, en opposition avec la recommandation de Rogers (2003) sur l'AS. En effet, cet auteur précise que le prestataire doit être vu « par les potentiels adoptants comme n'ayant pas d'intérêt personnel significatif dans l'adoption ou dans le rejet de la nouvelle technologie » (en l'occurrence la mesure de sécurité, op. cit.). Ainsi, le prestataire contribue fortement à l'influence normative de la solution dans les deux dernières phases de l'AS (recueil d'information et évaluation de la solution). En perspective du principe de *satisficing* (March et Simon en 1958) le dirigeant peut alors être conduit à choisir une « première solution technique » qui **ne conviendrait que partiellement aux besoins de sécurité réels** (au sens de Doherty et Fulford 2006 et May 2003).

Enfin, notre dernière contribution relève **d'un modèle théorique innovant**, qui a permis d'éclairer la gestion des risques SI avec un cadre combinant le **processus de décision** et le traitement des **risques perçus**. En ce sens, rappelons que les travaux fondateurs pour la perception des risques de Slovic et al. (1984 p. 183) soulignent que « la recherche dans le cadre de la théorie de décision comportementale peut contribuer à bien des égards à la

gestion et à la régulation du risque ». Ainsi, nous avons pu mettre en perspective des risques SI, les apports d'une discipline établie et contribuer **à confirmer ou à relativiser certains constats de la littérature en SSI**. Spécifiquement à l'adoption symbolique de la SSI, nos résultats font émerger une **prise de conscience pour les risques potentiels** pouvant conduire à conclure que la SSI est une « bonne idée ». À la marge, nous notons que les risques vécus contribuent particulièrement à cette prise de conscience, davantage que les risques imaginés ou partagés (tels que présentés dans le paragraphe « 244 Les risques perçus » p. 244244). Ensuite, ces risques se traduisent justement par une déclinaison des conséquences possibles et des menaces redoutées. Enfin, notre cadre théorique a permis de mettre en exergue les influences, à **la fois sur le risque perçu et sur les mesures de sécurité pour le couvrir**. Parmi ces influences nous pointons le rôle majeur des conseillers spécialisés en SSI, autrement nommés les prestataires dans nos travaux, pouvant agir sur le risque perçu, le choix et la mise en œuvre des mesures de sécurité. Au-delà du périmètre de nos travaux, nous avons pu observer la dissonance du modèle d'adoption symbolique de Karahanna et al. (1999) et Rogers (1995) qui malgré une adoption symbolique de la SSI peut conduire à un **rejet de l'adoption réelle.**

En résumé, les dirigeants considèrent leur SI et la SSI comme importants en regard de l'activité adossée au SI. Ils énoncent ne pas pouvoir *« se passer »* de ce dernier. Ils présentent ainsi une aversion pour les risques qui pourraient mettre en défaut leur SI, eux-mêmes et, *in fine*, leur organisation. **La décision d'adopter la SSI s'appuie sur un processus où chaque étape peut être influencée par des caractéristiques idiosyncratiques (expériences, connaissances, objectifs et priorités) ou par des informations provenant de réseau d'influence et de prestataires « informatique ».** De plus, **les dirigeants établissent l'acceptation des risques SI sur la base de leur perception des risques dont la connaissance repose sur les conséquences redoutées, en ignorant leur exposition au risque**. Ainsi, la SSI devient « une bonne idée » dès lors que le risque couvert semble avoir des conséquences réduites et acceptables. Notre choix, de combiner plusieurs approches théoriques, contribue à faire émerger plusieurs connaissances pour rendre intelligible la décision des dirigeants quant à l'adoption matérielle potentielle de la SSI.

7.2. Les contributions managériales de la recherche

Notre projet de recherche s'inscrit dans la génération de connaissances applicables et pragmatiques pour les praticiens. Ainsi, nous proposons des contributions managériales

participant à l'adoption symbolique de la SSI. Dans cette perspective, nous orientons nos préconisations sur la finalité de la gestion du risque : **l'acceptation de risque objectivé et contrôlé**.

Nos résultats font clairement émerger l'intérêt des dirigeants pour la SSI. Les prises de conscience des risques possibles en sont une illustration. Cependant, nous notons une posture réactive pour l'adoption de mesure de sécurité en ce sens où il est parfois nécessaire qu'un risque devienne un sinistre, au sens de Kermisch (2012), pour engager une réflexion sur la mesure de sécurité qui aurait pu le contrer. Cette réactivité au risque SI pourrait être gommée selon deux préconisations mutuelles.

D'une part, la phase de recueil d'information conduit les dirigeants à observer les pratiques de leur entourage et de leur prestataire. Cette phase peut combiner une recherche d'information sur la SSI (au sens ISO/CEI 27001[87], 2013), ou sur la mise en œuvre d'une une mesure de protection seule. Cette dernière option ressort particulièrement de nos résultats et conduit alors à une approche centrée sur **une solution technique** (dont la sauvegarde représente le choix majoritaire dans nos résultats). Nous proposons alors de considérer, lors de cette phase, non pas une étude technique de la solution mais, une étude qui permettrait au dirigeant de disposer d'une vision globale des risques auxquels sont exposés le SI. En effet, rappelons que l'approche risque pour le SI, appelle l'identification et de la formulation de problèmes en ce qui concerne le risque SI, c'est-à-dire **une analyse de risque** (Albrechtsen et Hovden 2009 ; Bandyopadhyay et al. 1999 ; Choobineh et Dhillon 2007 ; Straub et Welke 1998). Ainsi, outre la formalisation « complétée » et méthodique du risque, **une vision globale des risques auxquels sont exposés le SI, faisant interagir menace, conséquence et probabilité, permettrait d'orienter leur traitement selon les spécificités des organisations et de leurs enjeux**. À l'inverse, rappelons que ne pas employer de méthode adaptée pour analyser les risques peut conduire à une sécurité réactive. Précisément, nos résultats montrent qu'écarter l'analyse des risques contribue à masquer les risques possibles pesant sur les activités majeures de l'organisation et, par là-même, à orienter la SSI sur les seuls aspects technologiques des SI (Bandyopadhyay et al. 1999 ; Choobineh et Dhillon 2007 ; Dlamini et al. 2009 ; Doherty et Fulford 2006 ; Kwon et Johnson 2014 ; Karyda et al. 2005 ; McFadzean et al. 2007 ; Vance et al. 2014).

[87] Que nous rappelons ici : « …préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate » ISO/CEI 27001 (2013) p. V

Cette approche technique de la SSI peut s'inscrire dans des adoptions successives de mesure de sécurité isolée, ce qui se traduirait par autant d'adoptions symboliques que de mesures choisies. Une SSI holistique et organisée (Bandyopadhyay et al. 1999 ; Posthumus et Solms 2004 : Soomro et al. 2016) relèverait alors d'une adoption symbolique ou la SSI est étudié globalement, au sens de l'ISO/CEI 27001 (2013), qui préserverait l'organisation de la survenance des risques ou permettant d'en limiter les conséquences défavorables, le cas échéant.

D'autre part, **l'exposition au risque n'émerge pas particulièrement de nos résultats**. Le point précédent est en accord avec la littérature issue du champ psychologique et permet de comprendre pourquoi les dirigeants ont tendance à sous-estimer les risques[88]. Selon nous, la préférence des évaluateurs pour aborder le risque par les menaces représente **un biais pouvant masquer une[89] réalité d'un risque**. Ainsi, pour faire écho aux propos de Loch et al. (1992 p. 185) qui précisent « croyance plutôt naïve que de mauvaises choses arrivent seulement aux autres » nous suggérons **d'étudier l'exposition du SI au risque**. En effet Willison et Backhouse (2006) soulignent que le risque SI peut s'aborder sous l'angle de l'étude des vulnérabilités, conduisant à analyser l'exposition au risque SI. En effet, rappelons que ces auteurs définissent le risque SI par une menace et une vulnérabilité. Cette préconisation permettrait à l'évaluateur de dépasser son sentiment de contrôle du risque SI (Cadet et Kouabénan 2005 ; Chauvin et Hermand 2006) et d'en disposer d'une vision objective (Kankanhalli et al. 2003).

Deuxièmement, dans le prolongement de l'exposition au risque, nous préconisons aux réseaux d'influences professionnels, regroupant les syndicats, clubs et professionnels du domaine, de **communiquer sur le risque en abordant celui-ci dans son ensemble et non pas seulement par la menace**. En effet, une communication centrée sur les impacts possibles sur l'organisation et les dirigeants, ainsi que sur l'exposition du SI, nous semble adaptée. Précisément, nous voyons dans cette approche de la communication du risque un moyen d'influencer et de changer les croyances et les attitudes des directeurs pour la SSI (Hu

[88] Pour illustrer ce propos, s'agissant d'un risque de « piratage », nous pouvons ici citer Robert Muller, Directeur du FBI, qui précisait en 2012 : « Je suis convaincu qu'il y a seulement deux types d'entreprises : celles qui ont été piratées et celles qui le seront. Et les deux convergeront dans une même catégorie : les entreprises qui ont été piratées et celles qui le seront à nouveau. (https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies)

[89] Notre posture épistémologique nous invite à considérer le risque comme un construit social (Slovic et al. 1982; Sjöberg et al. 2004) qui n'est que partiellement partagée entre expert et profane (Yates et Stone 1992), aussi nous préférons l'emploi de l'article indéfini

et al. 2007). La communication pourrait être élaborée par groupe de décideurs œuvrant dans des secteurs d'activité identiques et dans des structures d'organisation comparables. Cette recommandation s'inscrit dans une influence isomorphique mimétique, en accord avec le modèle de Straub et Welke (1998). Ces auteurs précisent qu'une des trois influences nécessaires pour investir la SSI repose sur la connaissance de « l'environnement organisationnel » soit « la connaissance des risques inhérents à une industrie spécifique » (Straub et Welke 1998 p. 444).

Troisièmement, comme nous en avons discuté précédemment, l'expression individuelle d'un risque est **contextuelle** (Slovic et al. 1979) et **situationnelle** (Sjöberg et al. 2004 ; Yates et Stone 1992). Ainsi nous suggérons de **renforcer la formation des dirigeants afin qu'ils puissent eux-mêmes apprécier et évaluer les risques SI**. En effet, nos résultats montrent l'influence des formations sur la décision d'adopter la SSI. Cette recommandation s'inscrit, d'une part, dans la perspective de la théorie culturelle du risque (Douglas et Wildavsky 1983 ; Rippl 2002 ; Sjöberg et al. 2004 ; Tansey et O'riordan 1999) partagée pour la SSI (Knapp et al. 2006 ; May 2003 ; Siponen 2000 ; Solms 2001a ; Hagen et al. 2008). En regard de la dépendance croissante des entreprises envers leur SI, il apparait tout à fait pertinent d'enseigner la culture du risque dans d'autres disciplines que celles traitant des systèmes d'information. En ce sens il s'agirait alors d'une influence isomorphique normative, comme le rappelle le commentaire sur la standardisation des cursus éducatifs, pouvant mener à partager des croyances semblables sur la « juste manière d'organiser » (Rizza 2008 p. 13).

En résumé, **l'approche de la SSI doit s'établir selon des principes méthodologiques permettant de formaliser les risques, c'est-à-dire les menaces et les conséquences, puis d'objectiver les probabilités de survenance de ces risques**. La communication et la transmission de l'analyse de risque des SI peut constituer une influence qui favoriserait la connaissance des risques et ainsi participerait à l'adoption de la SSI. Enfin, une communication sectorielle, adaptée à des groupes de dirigeants dont les problématiques SSI et les contextes organisationnels seraient comparables, contribuerait à objectiver l'exposition au risque et ainsi décider pertinemment de l'acceptation du risque.

7.3. Les limites de la recherche

Notre recherche présente les limites inhérentes au cadre théorique élaboré et à la méthodologie utilisée, ainsi qu'à la démarche qualitative suivie. Ces limites constituent

autant de pistes pour l'utilisation d'autres dispositifs d'études afin d'appréhender différemment la complexité du phénomène étudié.

Notre projet est inscrit dans une approche exploratoire et vise à rendre intelligible les influences considérées dans la décision, dans un contexte, pour un dirigeant et une situation donnée. Les cas étudiés n'offrent qu'un nombre limité d'illustrations possibles des influences et de leurs interactions pour l'adoption symbolique de la SSI. Dans le respect de notre épistémologie et d'une démarche de recherche qualitative, nos travaux ne prétendent pas une généralisation statistique à un échantillon plus large. Il s'agit davantage d'une généralisation conceptuelle qui amène à développer des connaissances dites « génériques » au sens d'Avenier et Gavard-Perret (2012). Ces auteures rappellent que l'élaboration de ces connaissances repose sur un travail préliminaire de catégorisation par comparaison de diverses manifestations du phénomène étudié et d'identification de leurs similarités et de leurs disparités (op. cit.). Nous avons combiné plusieurs approches théoriques, pour rendre intelligible la décision des dirigeants. En vue d'une démarche d'analyse de contenu nous avons fait ensuite émerger de ce corpus théorique différentes catégories au sens la « valeur d'un thème » (Thiétart et al. 2003 p. 463). La question de validité, qui, selon Miles et Huberman (2003 p. 78) repose sur les compétences du chercheur, peut être posée. Si deux chercheurs ont contribué à l'élaboration du guide d'entretien, nous n'avons pas jugé pertinent d'effectuer un double codage.

La fiabilité de la recherche qualitative repose principalement sur la « capacité et l'honnête du chercheur » (Thiétart et al. 2003 p. 277). Nous avons été présentés aux dirigeants interviewés comme « consultant et chercheur spécialisé en SSI ». Il semble alors que nous ayons effectivement influencé le recueil d'information (Gavard-Perret 2012), tels que les verbatims le montrent, conduisant les interviewés à s'interroger sur leur expositions aux risques ou à prononcer sur un jugement de valeur de leur niveau effectif de sécurité (cf. « 5.6 Commentaires des interviewés lors des entretiens » p. 308).

Notre échantillon, s'il n'est composé que de 17 entretiens, correspond aux critères de Miles et Huberman (2003). D'une part, ses caractéristiques permettent de « porter » la connaissance de notre étude de cas. Les verbatims montrent que tous les dirigeants ont pu se prononcer sur les thèmes abordés. D'autre part, la structure de cet échantillon permet de « découvrir » les construits sous-jacents à nos travaux. Enfin, il s'agit d'un échantillon à variation « maximale » en ce sens où les secteurs d'activités des interviewés sont particulièrement variés (Miles et Huberman 2003 p. 61). Enfin, si la taille de l'échantillon

peut être discutée, les derniers entretiens n'ont pas permis d'apporter d'éléments nouveaux, signifiant alors une possible saturation théorique.

Le modèle théorique d'adoption symbolique adapté à la SSI est décliné des travaux de Klonglan et Coward (1970) qui s'inscrivent dans la théorie de la diffusion d'innovation (Roger 1962). Un des intérêts majeurs de ce modèle est qu'il permet d'étudier l'acceptation d'une « idée », en **s'affranchissant des contraintes économiques et pratiques** qui surviennent lors de l'adoption matérielle. Notre étude exploratoire ne vise pas à tester l'adéquation de ce modèle à la décision pour la SSI, mais uniquement à contribuer à l'intelligibilité des influences sur cette décision.

7.4. Les voies de recherche

Les recherches futures pourraient éprouver la validité du modèle théorique d'adoption symbolique soit en utilisant un autre dispositif pour les étudier soit en limitant le périmètre d'étude à un secteur d'activité défini. D'une part il s'agirait d'apprécier la validité du modèle d'adoption symbolique adapté à la SSI. Ce modèle comprend les concepts issus du champ psychologique de perception des risques et des théories néo-institutionnalistes dont il faudrait vérifier l'adéquation au modèle. D'autre part, des applications à des secteurs d'activité particuliers permettraient de vérifier les effets sectoriels.

Ensuite, nous avons limité nos travaux à l'adoption symbolique de façon à s'affranchir des contraintes économiques et pratiques liées à la mise en œuvre. Prolonger ces travaux pourrait consister, pour un même cas, à mettre en perspective l'adoption symbolique et l'adoption matérielle. Cela contribuerait à enrichir la connaissance sur les entreprises où la SSI est réactive.

Une étude approfondie sur les raisons conduisant les évaluateurs du risque SI à écarter la probabilité de survenance, ou autrement dit, leur exposition au risque pourrait contextualiser, pour la SSI, les conclusions de la littérature du champ psychologique.

Afin de faciliter l'accès aux décideurs des organisations analysées, nous avons fait le choix d'étudier des TPE. Un prolongement de ces travaux à des entreprises de taille plus conséquente permettrait de donner une autre perspective à nos résultats. Ensuite, il pourrait porter un éclairage nouveau sur une éventuelle divergence entre top-managers et managers (cf. Choobineh et al. 2007).

Bibliographie

A

Abrams, M., & Bailey, D. (1995). Abstraction and refinement of layered security policy. Information Security: An Integrated Collection of Essays, 126-136.

Alhakami, A. S., & Slovic, P. (1994). A psychological study of the inverse relationship between perceived risk and perceived benefit. Risk analysis, 14(6), 1085-1096.

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. MIS quarterly, 665-694.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & security, 26(4), 276-289.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476-490.

Amalberti, R. (1996). La Conduite de systèmes à risques, Paris, puf, coll. Le travail humain, 3.

Anderson, J. M. (2003). Why we need a new definition of information security. Computers & Security, 22(4), 308-313.

Avenier, M. J. (2011). Les paradigmes épistémologiques constructivistes: post-modernisme ou pragmatisme?. Management & avenir, (3), 372-391.

Avenier, M. J., & Gavard-Perret, M. L. (2012). Inscrire son projet de recherche dans un cadre épistémologique (No. halshs-00355392).

Avenier, M. J., & Thomas, C. (2015). Finding one's way around various methodological guidelines for doing rigorous case studies: A comparison of four epistemological frameworks. Systèmes d'information & management, 20(1), 61-98.

B

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. European journal of information systems, 5(1), 2-9.

Bagchi, K., & Udo, G. (2003). An analysis of the growth of computer and Internet security breaches. Communications of the Association for Information Systems, 12(1), 46.

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. Management Decision, 37(5), 437-445.

Barlette, Y. (2012). Implication et action des dirigeants: quelles pistes pour améliorer la sécurité de l'information en PME? Systèmes d'information & management, 17(2), 115-149.

Barlette, Y., & Fomin, V. V. (2010). The adoption of information security management standards. Information resources management: concepts. Methodologies, tools and applications. IGI Global, Pennsylvania, 69-90.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. ACM Computing Surveys (CSUR), 25(4), 375-414.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15*(5/6), 337-346.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. Information & management, 51(1), 138-151.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. V. (2013). Digital business strategy: toward a next generation of insights. MIS Quarterly Vol. 37 No. 2, pp. 471-482

Bishop, M. (2003). *Computer security: art and science*. Addison-Wesley Profession

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151-164.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

C

Cadet, B., & Kouabénan, D. R. (2005). Évaluer et modéliser les risques: apports et limites de différents paradigmes dans le diagnostic de sécurité. Le travail humain, 68(1), 7-35.

Calvez, M. (2006). L'analyse culturelle de Mary Douglas: une contribution à la sociologie des institutions. SociologieS.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of ITSecurity Management: Four Improvements to Current Security Practices. The Communications of the Association for Information Systems, 14(1), 37.

Chang, S., & Lin, C. S. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438-458.

Charreire, S., & Huault, I. (2001). Le constructivisme dans la pratique de recherche: une évaluation à partir de seize thèses de doctorat. Finance contrôle stratégie, 4(3), 31-55.

Chauvin, B., & Hermand, D. (2006). Influence des variables distales sur la perception des risques: une revue de la littérature de 1978 à 2005. Les Cahiers internationaux de psychologie sociale, (4), 65-83.

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of information security: Challenges and research directions. Communications of the Association for Information Systems, 20(1), 57.

CLUSIF (2014) – Rapport sur les menaces informatiques et pratiques de sécurité en France https://clusif.fr/publications/menaces-informatiques-et-pratiques-de-securite-en-france-edition-2014/

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. computers & security, 32, 90-101.

D

Dake, K. (1992). Myths of nature: Culture and the social construction of risk. Journal of Social issues, 48(4), 21-37.

Dagorn, N. (2012). Le management de la sécurité de l'information : un état de l'art. In *17ème Colloque de l'AIM du 21 au 23 mai 2012 à Bordeaux*.

Dagorn, N., & Poussing, N. (2012). Engagement et pratiques des organisations en matière de gouvernance de la sécurité de l'information. Systèmes d'information & management, 17(1), 113-143.

David, A. (1999, May). Logique, épistémologie et méthodologie en sciences de gestion. In Conférence de l'AIMS (pp. 1-23).

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. Management science, 35(8), 982-1003.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, 20(1), 79-98.

Da Veiga, A., & Eloff, J. H. (2007). An information security governance framework. Information Systems Management, 24(4), 361-372.

Dhillon, G., & Backhouse, J. (1994, September). The use of information technology in organisations: dealing with systemic opportunities and risks. In The Second SISnet Conference (pp. 26-28).

Dhillon, G., & Backhouse, J. (1996). Risks in the use of information technology within organizations. *International Journal of Information Management*, *16*(1), 65-74.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. Communications of the ACM, 43(7), 125-128.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314.

Di Maggio, P., & Powell, W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147-160.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. Computers & Security, 28(3), 189-198.

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: an exploratory analysis. *Information Resources Management Journal (IRMJ)*, *18*(4), 21-39.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. Computers & Security, 25(1), 55-63.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. International journal of information management, 31(3), 201-209.

Douglas, M. (1978), "Cultural bias", Occasional Paper No. 35, Royal Anthropological Institute of Great Britain and Ireland.

Douglas, M., & Wildavsky, A. (1982). How can we know the risks we face? Why risk selection is a social process 1. Risk analysis, 2(2), 49-58.

Douglas, M., & Wildavsky, A. (1983). Risk and culture: An essay on the selection of technological and environmental dangers. Univ of California Press.

Dumez, H. (2011). Qu'est-ce que la recherche qualitative?. *Le Libellio d'Aegis*, *7*(4-Hiver), 47-58

E

Edwards, W. (1961). Behavioral decision theory. Annual review of psychology, 12(1), 473-498.

Eloff, J. H. (1988). Computer security policy: Important issues. Computers & Security, 7(6), 559-562.

Eloff J., Eloff M., 2003, Information Security Management - A New Paradigm, SAICSIT pp 130–136

Eloff, M. M., & von Solms, S. H. (2000). Information security management: a hierarchical framework for various approaches. Computers & Security, 19(3), 243-256.

EMC 2014, Key findings from the 2014 US State of Cybercrime, http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

EMC 2015, Key findings from the 2015 US State of Cybercrime Survey, http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf

F

Feldman, M. S., & March, J. G. (1981). Information in organizations as signal and symbol. *Administrative science quarterly*, 171-186.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research.

Fichman, R. G. (2001). The role of aggregation in the measurement of IT-related organizational innovation. MIS quarterly, 427-455

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. Journal of behavioral decision making, 13(1), 1.

Fischhoff, B. (1979). Informed consent in societal risk—benefit decisions. Technological Forecasting and Social Change, 13(4), 347-357.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. Policy sciences, 9(2), 127-152.

Fischhoff, B., Slovic, P., & Lichtenstein, S. (1979). Weighing the Risks: Risks: Benefits which Risks are Acceptable?. Environment: Science and Policy for Sustainable Development, 21(4), 17-38.

Fischhoff, B., Slovic, P., & Lichtenstein, S. (1979). Weighing the Risks: Risks: Benefits which Risks are Acceptable? Environment: Science and Policy for Sustainable Development, 21(4), 17-38.

Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S. L., & Keeney, R. L. (1981). Acceptable Risk. Cambridge : Cambridge University Press.

Fischhoff, B. (1985). Managing risk perceptions. Issues in Science and Technology, 2(1), 83-96.

Fomin, V. V., Vries, H., & Barlette, Y. (2008, September). ISO/IEC 27001 information systems security management standard: Exploring the reasons for low adoption. In EUROMOT 2008 Conference, Nice, France.

Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. Information Management & Computer Security, 11(3), 106-114.

G

Gavard-Perret, M. L., Gotteland, D., Haon, C., & Jolibert, A. (2008). Méthodologie de la recherche: réussir son mémoire ou sa thèse en sciences de gestion (No. halshs-00355220).

Gavard-Perret, M. L., Gotteland, D., Haon, C., & Jolibert, A. (2012). Méthodologie de la recherche en sciences de gestion. *Réussir son mémoire ou sa thèse*, 11-62

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. Computers & Security, 24(1), 16-30.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: a study of perceptions of the adequacy of security. Information & Management, 20(1), 13-27.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 5(4), 438-457.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). 2005 CSI/FBI computer crime and security survey. Computer Security Journal, 21(3), 1.

Guba, E. G., & Lincoln, Y. S. (1989). Fourth generation evaluation. Sage.

H

Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security, 16(4), 377-397

Haller, C. (2014). *Développement et valorisation des routines d'échanges d'informations au sein du territoire vitivinicole provençal: l'effectuation comme approche intégrative* (Doctoral dissertation, Thèse de doctorat en sciences de gestion, Aix Marseille Université).

Hameed, M. A., Counsell, S., & Swift, S. (2012). A conceptual model for the process of IT innovation adoption in organizations. Journal of Engineering and Technology Management, 29(3), 358-390.

Henderson, J. C., & Venkatraman, N. (1992). Strategic alignment: a model for organizational transformation through information technology. Transforming organizations, 97-117.

Herath, T., and Rao, H. G. 2009a "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," European Journal of Information Systems (18:2), pp. 106-125.

Herath, T., and Rao, H. R. 2009b "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", Decision Support Systems, 47(2), 154–165

Hermand, D., & Chauvin, B. (2008). Contribution du paradigme psychométrique à l'étude de la perception des risques: une revue de littérature de 1978 à 2005. L'Année psychologique, 108(2), 343-386.

Hogarth, R. M. (1980). Judgment and Choice. New York : Wiley.

Höne K., Eloff JHP., 2002a, An Information security policy – what do international security standards say ? Computers & Security ; Vol.21 No5 pp 402–409

Höne K., Eloff JHP., 2002b, What makes an Effective Information Security Policy? Network Security, Vol.6 pp. 14-16.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security–a neo-institutional perspective. The Journal of Strategic Information Systems, 16(2), 153-172.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees?. Communications of the ACM, 54(6), 54-60

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660.

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221-232.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. Information security technical report, 13(4), 247-255.

I

ISO/IEC 27000 (2016) Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Vue d'ensemble et vocabulaire

ISO/CEI 27001 (2013) Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information – Exigences

ISO/CEI 27005 (2011) Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information

I

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. Communications of the ACM, 52(1), 126-129.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS quarterly, 549-566

K

Kahneman, D., & Slovic, P. (1982). Amos Tversky, eds. 1982

Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. American economic review, 93(5), 1449-1475.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. International journal of information management, 23(2), 139-154.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. Computers & Security, 24(3), 246-260.

Karahanna, E (1997). "Symbolic Adoption of Information Technology," submitted to the Special Issue on Diffusion and Infusion of Information Technology, Information Resources Management Journal.

Karahanna, E. (1999). Symbolic Adoption of Information Technology. In Proceedings of Decision Sciences International Conference, Athens, Greece

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. MIS quarterly, 183-213.

Karahanna, E., & Agarwal, R. (2006). When the spirit is willing: Symbolic adoption and technology exploration. *University of Georgia, Athens, GA*.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. MIS Quarterly Executive, 9(3), 163-175.

Kermisch, C. (2010). Les Paradigmes de la perception du risque.

Kermisch, C (2011). Le concept du risque. De l'épistémologie à l'éthique

Kermisch, C. (2012). Vers une définition multidimensionnelle du risque. [VertigO] La revue électronique en sciences de l'environnement, 12(2).

Klonglan, G. E., & Coward, E. W. (1970). The concept of symbolic adoption: A suggested interpretation. Rural Sociology, 35(1), 77.

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. Information Management & Computer Security, 14(1), 24-36.

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers & Security, 28(7), 493-508.

Kouabenan, D. R. (2007). Incertitude, croyances et management de la sécurité. Le travail humain, 70(3), 271-287.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. Information & Management, 41(5), 597-607.

Kuhn, T. (1962) The structure of Scientific Revolutions, University of Chigaco Press.

Kwon, J., Ulmer, J. R., & Wang, T. (2012). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, *27*(1), 219-236

Kwon, J., & Johnson, M. E. (2014). Proactive vs. reactive security investments in the healthcare sector. Manage Inf Syst Q, 38(2), 451-471.

L

Le Breton, D. (2012). Sociologie du risque:«Que sais-je?» n° 3016. Presses universitaires de France.

Le Moigne, J. L. (2012). *Les épistémologies constructivistes:« Que sais-je? » n 2969*. Presses universitaires de France.

Lesca, N., Caron-Fasan, M. L., Aguirre, E. L., & Chalus-Sauvannet, M. C. (2015). Drivers and barriers to pre-adoption of strategic scanning information systems in the context of sustainable supply chain. Systèmes d'information & management, 20(3), 9-46.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. MIS quarterly, 59-87.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. MIS quarterly, 71-90.

Lichtenstein, S., Slovic, P., Fischhoff, B., Layman, M., & Combs, B. (1978). Judged frequency of lethal events. *Journal of experimental psychology: Human learning and memory*, *4*(6), 551

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. MIS Quarterly, 173-186.

M

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: a parsimonious framework. Information Management & Computer Security, 16(3), 251-270.

Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An integrated framework for information security management. Review of Business, 30(1), 58.

Magne, L. (2010). Histoire sémantique du risque et de ses corrélats. In Journées d'histoire de la comptabilité et du management.

May, C. (2003). Dynamic corporate culture lies at the heart of effective security strategy. Computer Fraud & Security, 2003(5), 10-13.

McFadzean, E., Ezingeard, J. N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. Online Information Review, 31(5), 622-660.

Moulton, R., & Coles, R. S. (2003). Applying information security governance. Computers & Security, 22(7), 580-584.

Miles, M. B., & Huberman, A. M. (2003). Analyse des données qualitatives. De Boeck Supérieur.

Mitchell, V. W. (1995). Organizational risk perception and reduction: a literature review. British Journal of Management, 6(2), 115-133.

N

Nah, F. F. H., Tan, X., & Teh, S. H. (2004). An empirical investigation on end-users' acceptance of enterprise systems. Information Resources Management Journal (IRMJ), 17(3), 32-53.

P

Pahnila, S., Karjalainen, M., & Siponen, M. T. (2013). Information Security Behavior: Towards Multi-Stage Models. In PACIS (p. 102).

Peltier, T. R. (2004). Developing an enterprisewide policy structure. Information Systems Security, 13(1), 44-50.

Peretti-Watel, P. (2000). Sociologie du risque. A. Colin.

Peretti-Watel, P. (2003). Risque et innovation: un point de vue sociologique. Innovations, (2), 59-72.

Peppard, J., & Ward, J. (2004). Beyond strategic information systems: towards an IS capability. The Journal of Strategic Information Systems, 13(2), 167-194.

Peppard, J., Galliers, R. D., & Thorogood, A. (2014). Information systems strategy as practice: Micro strategy and strategizing for IS. J. Strategic Inf. Sys., 23(1), 1-10.

Piaget, J. (1967). Logique et connaissance scientifique. Encyclopédie de la Pléiade.

Popper, K. (1991) La connaissance objective, Flammarion, 2ème édition française, 1ère édition en 1972, Paris

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), 638-646.

PWC 2016, Key findings from The Global State of Information Security Survey 2016(plus de 10 000 responsables interrogés dans 127 pays) https://www.pwc.com/ee/et/publications /pub/pwc-global-state-of-information-security-survey-20.pdf

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. Mis Quarterly, 757-778.

R

Rai, A., Brown, P., Tang, X. (2009), "Organizational assimilation of electronic procurement innovations", Journal of Management Information Systems, Vol. 26, nº1, p. 257–296.

Rawstorne, P., Jayasuriya, R., & Caputi, P. (1998, December). An integrative model of information systems use in mandatory environments. In Proceedings of the international conference on Information systems (pp. 325-330). Association for Information Systems

Reix, R., Fallery, B., Kalika, M., & Rowe, F. (2011). Systèmes d'information et management. Vuibert, Paris.

Richardson, R., & Director, C. S. I. (2008). CSI computer crime and security survey. Computer Security Institute, 1, 1-30.

Rippl, S. (2002). Cultural theory and risk perception: a proposal for a better measurement. Journal of risk research, 5(2), 147-165.

Rizza, R. (2008). Néo-institutionnalisme sociologique et nouvelle sociologie économique: quelles relations?. Revue Interventions économiques. Papers in Political Economy, (38).

Rogers, Everett M. (1962). Diffusion of Innovations New York : The Free Press

Rogers, Everett M. (1968). A communication research approach to the diffusion of innovations » Pp. 27-30 in Diffusino Research Needs. Columbia : Missouri Agricultural Experiment Station, North Central Region Research Bulletin 186.

Rogers EM (1983). Diffusion of Innovations (3rd edition). London: The Free Press.

Rogers, E. M. (2003). The diffusion of innovation 5th edition.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

S

Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. MIS quarterly, 237-263.

Sapp, S. G., & Korsching, P. F. (2004). The social fabric and innovation diffusion: Symbolic adoption of food irradiation. Rural Sociology, 69(3), 347-369.

Scott, W.R. (1995), Institutions and Organizations, Sage, Thousand Oaks, CA.

Scott, W. R. (2005). Institutional theory: Contributing to a theoretical research program. Great minds in management: The process of theory development, 37, 460-484.

Short, J. F. (1984). The social fabric at risk: toward the social transformation of risk analysis. American sociological review, 49(6), 711-725.

Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. Information Management & Computer Security, 22(3), 279-308

Simon, H.A. (1996) The sciences of the artificial, 3e édition, Cambridge, The Mit Press

Siponen, M. T. 2000. "A Conceptual Foundation for Organizational Information Security Awareness," Information Management and Computer Security (8:1), pp. 31-41.

Siponen, M. T. (2005). An analysis of the traditional IS security approaches: implications for research and practice. European Journal of Information Systems, 14(3), 303-315.

Siponen, M. & Iivari, J. (2006). Six design theories for IS security policies and guidelines. Journal of the Association for Information systems, 7(1), 19.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 38(1), 60-80

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 487-502.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270.

Sjöberg, L. (2000). Factors in risk perception. *Risk analysis*, *20*(1), 1-12.

Sjöberg, L. (2002). The allegedly simple structure of experts' risk perception: an urban legend in risk research. Science, Technology, & Human Values, 27(4), 443-459.

Sjöberg, L., Moen, B. E., & Rundmo, T. (2004). Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research, 33.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1980). Facts and fears: Understanding perceived risk. In Societal risk assessment (pp. 181-216). Springer, Boston, MA.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1982). Why study risk perception?. Risk analysis, 2(2), 83-93.

Slovic, P., Lichtenstein, S., & Edwards, W. (1965). Boredom-induced changes in preferences among bets. The American journal of psychology, 78(2), 208-217.

Slovic, P. (1992). Perception of risk: Reflections on the psychometric paradigm.

Slovic, P. (1999). Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield. Risk analysis, 19(4), 689-701.

Slovic, P. E. (2000). The perception of risk.

Slovic, P. (2016). The perception of risk. Routledge.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1979). Rating the risks. Environment: Science and Policy for Sustainable Development, 21(3), 14-39.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1980). Facts and fears: Understanding perceived risk. In *Societal risk assessment* (pp. 181-216). Springer, Boston, MA.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1982a). Why study risk perception?. Risk analysis, 2(2), 83-93.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1982b). Facts versus fears : Understanding perceived risk. In D. Kahneman, P. Slovic, & A. Tversky (Eds.), Judgment under Uncertainty : Heuristics and Biases (pp. 463-489). Cambridge : Cambridge University Press.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1984). Behavioral decision theory perspectives on risk and safety. Acta psychologica, 56(1), 183-203.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1985). Characterizing perceived risk.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1986). The psychometric study of risk perception. In Risk evaluation and management (pp. 3-24). Springer, Boston, MA.

Slovic, P., Fischhoff, B., & Lichtenstein, S (1987). Perception of risk. Science, 236(4799), 280-285.

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. Risk analysis, 24(2), 311-322

Slovic, P., & Peters, E. (2006). Risk perception and affect. *Current directions in psychological science*, *15*(6), 322-325.

Solms, R., Van Der Haar, H., Solms, S. H., & Caelli, W. J. (1994). A framework for information security evaluation. Information & Management, 26(3), 143-153.

Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, *7*(1), 50-58.

Solms, B. (2000). Information security—the third wave? Computers & Security, 19(7), 615-620.

Solms, B. (2001a). Corporate governance and information security. Computers & Security, 20(3), 215-218.

Solms, B. (2001b). Information security—a multidimensional discipline. Computers & Security, 20(6), 504-508.

Solms, B. (2006). Information security–the fourth wave. Computers & security, 25(3), 165-168.

Solms, R., & Solms, B. (2004a). From policies to culture. Computers & security, 23(4), 275-279.

Solms, B., & Solms, R. (2004b). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376.

Solms, S. B. (2005). Information Security Governance–compliance management vs operational management. Computers & Security, 24(6), 443-447.

Solms, R. (1996). Information security management: The second generation. Computers & Security, 15(4), 281-288.

Solms, B., & Solms, R. (2005). From information security to… business security?. *Computers & Security*, *24*(4), 271-273.

Solms, R., & Solms, S. B. (2006a). Information Security Governance: a model based on the direct–control cycle. Computers & Security, 25(6), 408-412.

Solms, R., & Solms, S. B. (2006b). Information security governance: Due care. *Computers & Security*, *25*(7), 494-497.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Son, J. Y., & Benbasat, I. (2007). Organizational buyers' adoption and use of B2B electronic marketplaces: efficiency-and legitimacy-oriented perspectives. Journal of management information systems, 24(1), 55-99.

Sowby, F. D. (1965). Radiation and other risks. Health Physics, 11(9), 879-887.

Spears, J. L. (2007). Institutionalizing information security risk management: A multi-method empirical study on the effects of regulation. ProQuest.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. MIS Quarterly, 503-522.

Starr, C. (1969). Social benefit versus technological risk. Science, 1232-1238.

Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276.

Straub Jr, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS quarterly*, 45-60.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. MIS Quarterly, 441-469.

Sun, L., Srivastava, R. P., & Mock, T. J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. Journal of Management Information Systems, 22(4), 109-142.

Swanson, E. B., & Ramiller, N. C. (2004). Innovating mindfully with information technology. MIS quarterly, 553-583.

T

Tansey, J., & O'riordan, T. (1999). Cultural theory and risk: a review. Health, risk & society, 1(1), 71-90.

Taylor, R. (2006). Management perception of unintentional information security risks. ICIS 2006 Proceedings, 95.

Taylor, R. G. (2015). Potential problems with information security risk assessments. Information Security Journal: A Global Perspective, 24(4-6), 177-184.

Thiétart et al. (2003), Méthodes de recherche en Management, Paris, Dunod, 2ème édition.

Triandis, H. C. (1971). Attitude and attitude change. John Wiley & Sons.

Triandis, H. C. (1979). Values, attitudes, and interpersonal behavior. In Nebraska symposium on motivation. University of Nebraska Press.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2006). Formulating information systems risk management strategies through cultural theory. Information Management & Computer Security, 14(3), 198-217.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive psychology*, *5*(2), 207-232

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty : Heuristics and biases. Science, 185, 1124-1131.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. Science, 211(4481), 453-458.

V

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security, 29(4), 476-486.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). Journal of the Association for Information Systems, 15(10), 679.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management science, 46(2), 186-204.

Verra, L., Karoui, M., & Dudezert, A. (2012, May). Adoption symbolique d'un Réseau Social pour entreprise: Le cas de BOUYGUES CONSTRUCTION. In 17ème Conférence Internationale de l'Association Information et Management (AIM) (p. 23)

Von Glasersfeld, E., (1988), « Introduction à un constructivisme radical », in Paul Watzlawick, (dir.), L'invention de la réalité, Paris, Seuil, pp. 19-43.

Vitale, M. R. (1986). The growing risks of information systems success. MIS Quarterly, 327-334.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191-198.

W

Wacheux, F. (1996). Méthodes qualitatives et recherche en gestion. Economica.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems, 18(2), 101-105.

Watzlawick, P. (1988). L'invention de la réalité. Contribution au Constructivisme. Paris: Seuil

Whitman, M. E. (2003). Enemy at the gate: threats to information security. Communications of the ACM, 46(8), 91-95

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. International Journal of Information Management, 24(1), 43-57.

Whitman ME, Mattord HJ. Principles of information security. 3rd ed. Thompson Course Technology; 2009.

Whitman, M. E., & Mattord, H. J. (2016). Threats to Information Protection-Industry and Academic Perspectives: An annotated bibliography. Journal of Cybersecurity Education, Research and Practice, 2016(2), 4.

Wilde, Gerald J. S. (01.12.1982). The Theory of Risk Homeostasis: Implications for Safety and Health. Risk analysis. (2)4. p.209 – 225

Wildavsky, A., & Dake, K. (1990). Theories of risk perception: Who fears what and why?. *Daedalus*, 41-60.

Williams, Z., Lueg, J. E., Taylor, R. D., & Cook, R. L. (2009). Why all the changes? An institutional theory approach to exploring the drivers of supply chain security (SCS). International Journal of Physical Distribution & Logistics Management, 39(7), 595-618

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. Information and organization, 16(4), 304-324.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. European Journal of Information Systems, 15(4), 403-414.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS quarterly, 37(1).

Wood, C. C. (1995). Writing infosec policies. Computers & Security, 14(8), 667-674.

Y

Yates, J. F., & Stone, E. R. (1992). The risk construct.

Yin, R. K. (1989). Case Study Research (rev. ed)

Z

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. Communications of the Association for Information Systems, 24(1), 34.

Table des matières

Résumé **4**

Abstract **5**

Remerciements **6**

Sommaire **7**

Chapitre 1. Introduction générale de la recherche **9**

1.1. Contexte et objet de la recherche 9

1.1.1. Les systèmes d'information 9

1.1.2. La protection des SI 11

1.1.3. Le management de la sécurité de l'information 13

1.1.4. Positionnement de notre recherche et problématique 16

1.2. Contributions et organisation de la recherche 20

1.2.1. Contributions académiques et managériales 20

1.2.2. Posture épistémologique, Méthodologie et Protocole de la recherche 23

1.2.3. Organisation de la recherche 24

Chapitre 2. État de l'art de la sécurité des SI **26**

2.1. Importance des SI 27

2.2. Sécurité du SI 30

2.3. Définitions du management de la sécurité de l'information 31

2.4. Principaux thèmes de la recherche en SSI 36

2.4.1. Gouvernance 41

2.4.2. Sécurité des systèmes d'information et management 49

2.4.3. Politique de sécurité des SI 55

Élaboration et adaptation à l'organisation 56

Implémentation et efficacité 58

2.4.4. Analyse de risque 61

Concept et apport pour la SSI : la gestion du risque SI 62

Les pratiques empiriques étudiées dans la littérature : plusieurs lacunes 65

Gestion des risques : décision et responsabilités pour la SSI 67

2.4.5. Conformité 70
Conformité aux règles SSI 71
Conformité réglementaire et légale 72
Normes, standards et risques 74
2.5. Prolongements théoriques de la recherche en SSI 76
2.5.1. Implication pour la SSI des dirigeants 76
2.5.2. Manque d'étude sur la perception des risques 79
2.5.3. Approche socio-organisationnelle 80
2.5.4. Application de la théorie néo-institutionnelle 82
2.6. Questions de recherche 82
2.7. Conclusion du chapitre 84
Chapitre 3. Cadre théorique pour l'adoption symbolique 88
3.1. Le modèle d'adoption symbolique 88
3.1.1. L'adoption symbolique : étude des décisions d'adoption d'innovation 90
3.1.2. Concepts sous-jacents de l'adoption symbolique 92
Première étape d'adoption symbolique : la conscience de l'innovation 95
Seconde étape d'adoption symbolique : renseignement sur l'innovation 96
Troisième étape d'adoption symbolique : l'évaluation de l'innovation 98
Décalage entre la phase d'adoption symbolique et la phase d'adoption d'usage 100
Adoption ou rejet symbolique 102
3.1.3. Intérêt du modèle d'AS pour nos travaux 103
3.2. Perception des risques 105
3.2.1. Définition du risque 106
3.2.2. Concepts de l'étude des risques 111
L'incertitude 111
Les conséquences 112
Le risque acceptable 114
3.2.3. L'utilité espérée 118
3.2.4. Le paradigme cognitif 123
3.2.5. Paradigme psychométrique 126
Dimension sociale des risques 128
Construction sociale du risque 130
L'évaluation psychométrique du risque 131
La théorie culturelle du risque 140

Perceptions et théorie culturelle des risques 148
Synthèse du paradigme psychométrique et de la théorie culturelle du risque 151
3.2.6. Les biais d'évaluation des risques 157
Disponibilité 157
Représentativité 159
Ancrage-ajustement 160
Effet de cadrage 161
Excès de confiance 162
L'insensibilité aux probabilités 164
3.2.7. Perception des risques et SSI 165
Loch et al. (1992), Réalité des menaces d'aujourd'hui, compréhension d'hier 166
Straub et Welke (1998), faire face aux risques, modèles de planification de sécurité pour les décisions de management 167
Taylor (2006), perception managériale des risques involontaires sur la sécurité de l'information 169
Tsohou et al. (2006), formulation de stratégies de gestion des risques SI par la théorie culturelle 171
Albrechtsen (2007), l'avis des utilisateurs sur la sécurité de l'information 172
McFadzean et al. (2007), perception des risques et impact de l'IT existante sur la stratégie de sécurité de l'information au niveau exécutif 174
Albrechtsen et Hovden (2009), le clivage entre managers SSI et les utilisateurs 179
Huang et al. (2010), perception de sécurité de l'information 181
Synthèse des travaux SSI sur la perception des risques 183
3.2.8. Synthèse du chapitre sur la perception des risques 185
3.3. Influences externes et internes 187
3.3.1. Isomorphisme coercitif 189
3.3.2. Isomorphisme normatif 190
3.3.3. Isomorphisme mimétique 192
3.4. L'adoption symbolique adaptée à la gestion du risque 193
3.4.1. Première étape : le besoin de protéger le SI 193
3.4.2. Seconde étape : comment gérer le risque SI 195
3.4.3. Troisième étape : évaluer la SSI en regard du besoin 196
3.5. Conclusion du chapitre 198
Chapitre 4. Épistémologie et choix méthodologiques 202
4.1. Épistémologie 204
4.1.1. Positivisme 208

4.1.2. Constructivismes 210
4.1.3. Posture épistémologique constructiviste pragmatique 216
4.2. Méthodologie 219
4.2.1. Choix de la méthode qualitative 220
4.2.2. Collecte et analyse des données 224
Entretiens 225
Analyse et codage 227
4.2.3. Rigueur du processus de recherche 231
Chapitre 5. Résultats de la recherche 234
5.1. Contexte : SI et SSI 235
5.1.1. Importance du SI 235
5.1.2. Importance de la SSI 237
5.1.3. Synthèse de l'importance des SI et de la SSI 241
5.2. Les risques pour le SI, le dirigeant et l'entreprise 244
5.2.1. Les risques perçus 244
Les risques perçus imaginés 244
Les risques perçus vécus personnellement 249
Les risques vécus par des proches 252
Les risques connus car « médiatisés » 254
5.2.2. Les menaces 256
Menaces et exposition 256
Les menaces exogènes 257
Les menaces endogènes 259
5.2.3. Les conséquences des risques 260
Les conséquences directes sur l'entreprise 261
Les conséquences « métier » 263
Les conséquences directes sur le dirigeant 264
Les conséquences techniques sur le SI 265
Les conséquences directes sur le client 265
5.2.4. Acceptation du risque 265
5.2.5. Synthèse des risques perçus, des menaces et des conséquences 267
5.3. Influences isomorphiques 278
5.3.1. Influences normatives 278
5.3.2. Influences coercitives 279

5.3.3. Influences mimétiques 282
5.3.4. Synthèse des influences isomorphiques 283
5.4. Éléments du processus de décision d'adoption symbolique 286
5.4.1. Perception des besoins 286
5.4.2. Renseignement sur la solution 291
5.4.3. Évaluation de la solution 295
5.4.4. Synthèse du processus d'adoption symbolique 298
5.5. Réponse pratique au risque, mise en œuvre de la SSI 303
5.5.1. Absence de mise en œuvre 303
5.5.2. Mise en œuvre 304
5.5.3. Compétences mobilisées 306
5.6. Commentaires des interviewés lors des entretiens 308
5.7. Synthèse des résultats de la recherche 310
Chapitre 6. Interprétations et discussions 314
6.1. Éléments considérés lors de la décision d'AS 315
6.1.1. L'importance des SI au cœur du regard sur la SSI 315
6.1.2. Des risques souvent définis partiellement 318
6.1.3. Des conséquences considérées selon plusieurs perspectives 321
Les conséquences directes sur l'entreprise et sur le dirigeant 321
Les conséquences « métier » 323
6.1.4. Une exposition à la menace peu objectivée 328
6.1.5. Différentes sources pour la connaissance des risques SI 331
6.1.6. Connaissance « isomorphique » des risques et de la SSI 333
6.1.7. Conclusion des influences sur la perception du risque SI 339
6.2. Les influences sur la décision d'AS 342
6.2.1. Perception des besoins 342
6.2.2. Renseignement sur la solution 346
6.2.3. Évaluation de la solution 350
6.2.4. Conclusion des influences sur la décision d'AS 352
Chapitre 7. Conclusion générale de la recherche 357
7.1. Les contributions théoriques de la recherche 358
7.2. Les contributions managériales de la recherche 362
7.3. Les limites de la recherche 365

7.4. Les voies de recherche.....367

Bibliographie 368

Table des matières.....388

Liste des figures 394

Liste des tableaux.....395

Annexes.....396

Liste des figures

Figure 1 : Trois étapes conduisant au rejet ou à l'adoption symbolique 19
Figure 2 : Problématique de la recherche 20
Figure 3 : Canevas général du projet de recherche 25
Figure 4 : Gouvernance et SSI, modèle de pilotage 37
Figure 5 : Thèmes de recherche SSI 41
Figure 6 : Modèle de planification pour traiter les risques SI 65
Figure 7 : Synoptique intermédiaire de notre recherche 87
Figure 8 : Formulation initiale du modèle TAM 89
Figure 9 : Place de l'AS dans le processus d'adoption 91
Figure 10 : Street calculus 110
Figure 11 : Influence de l'affect sur l'évaluation risque / bénéfices 117
Figure 12 : Modèle conceptuel du jugement 124
Figure 13.1 : Position des risques selon les 18 déterminants du risque 132
Figure 13.2 : Détail des déterminants sur les deux facteurs 133
Figure 14 : Résultats partiels des relations entre risques perçus et bénéfices perçus 137
Figure 15 : Typologie des modes de vies selon la théorie culturelle du risque 143
Figure 16 : Dépendance de référence dans la perception de luminosité 162
Figure 17 : Modèle des perceptions managériales des risques SI 168
Figure 18 : Rôles des membres exécutifs 175
Figure 19 : Grille de perceptions des risques et importance stratégique des SI 177
Figure 20 : Grille des déterminants qui peuvent influencer la perception des risques SI 182
Figure 21 : Adaptation du modèle d'AS à la SSI 197
Figure 22 : Six paradigmes épistémologiques 206
Figure 23 : Synthèse du design de recherche 220

Liste des tableaux

Tableau 1 : Définitions de la SSI identifiées dans la littérature 35
Tableau 2 : Thèmes de recherche développés dans la littérature 40
Tableau 3 : Synthèse des concepts mobilisés dans la littérature d'adoption symbolique..... 99
Tableau 4 : Synthèse des processus de pré-adoption dans la littérature SI 103
Tableau 5 : Déterminants du risque (Slovic 1982a ; 2000) 135
Tableau 6 : Résultats partiels des risques perçus et bénéfices perçus 136
Tableau 7 : Éléments clés des stratégies de gestion des risques SI.....151
Tableau 8 : Synoptique des hypothèses et principes du positivisme et constructivisme 212
Tableau 9 : Synoptique des hypothèses et principes des constructivismes 215
Tableau 10 : Limites et particularités de la recherche qualitative 224
Tableau 11 : Objectif des thèmes en regard des questions.....226
Tableau 12 : Idées reçues sur les données primaires 228
Tableau 13 : Codage des thèmes.....231
Tableau 14 : Synthèse des verbatims sur l'importance des SI et de la SSI 243
Tableau 15 : Synthèse des verbatims sur les risques pour le SI, le dirigeant et l'entreprise.277
Tableau 16 : Synthèse des verbatims sur les influences isomorphiques.....285
Tableau 17 : Synthèse des éléments du processus d'adoption symbolique 302
Tableau 18 : Synthèse des résultats de la recherche.....313
Tableau 19 : Synthèse de la nature et de l'origine des besoins en SSI 356

Annexes

Liste des annexes

- Revues mobilisées pour la synthèse des thèmes SSI
- Thèmes mobilisés par Zafar et Clark (2009)
- Biais culturels et éléments de langage
- Guide d'entretien et sources des questions
- Monographie des entreprises des dirigeants interviewés
- Entretien avec D11

Revues mobilisées pour la synthèse des thèmes SSI

	Zafar et Clark (2009) Top 10% du classement des 50 meilleures revues classées	Zafar et Clark (2009) Senior Scholars Basket (2006)	Silic et Back 2014
MIS Quarterly (MISQ)	X	X	X
Information Systems Research (ISR)	X	X	X
Journal of Management Information Systems (JMIS)	X	X	
European Journal of Information Systems (EJIS)	X	X	X
Information & Management (I & M)	X		X
Communications of the Association for Information Systems (CAIS)	X		
Journal of AIS (JAIS)			
Information Systems Journal (ISJ)		X	X
Journal of Information Technology (JIT)			X
Journal of MIS (JMIS)			X
Journal of Strategic Information Systems (JSIS).			X

Thèmes mobilisés par Zafar et Clark (2009)

Security theme	Assessment
Governance	Strategy and Information
	Security Policy
	Security Compliance
	Security Risk Management
	Governance Structure
	Information Security Advisory
Privacy	Policy, Practices and Controls
	Privacy and Information
	Management Strategy
	Data, Rules, and Objects
Threat	Mitigation
	Network Segmentation and
	Boundary Protection
	Vulnerability Management
	Content Checking
	Incident Management
Transaction and Data Integrity	Business Process Transaction
	Security
	Database Security
	Message Protection
	Secure Storage
	Systems Integrity
Identity and Access Management	Identity Proofing
	Access Control
	Identity Lifecycle Management
Application Security	Systems Development Life
	Cycle
	Application Development
	Environment
Physical Security	Site Management Physical
	Asset Management
Personnel Security	Workforce Security

Biais culturels et éléments de langage

Adapté pour la théorie culturelle du risque selon Rippl (2002 p. 164) et les travaux de Dake (1992) :

A- Hiérarchiste

1) Nous devrions disposer de forces armées plus puissantes que celles que nous avons
2) Je pense que la jeunesse devrait faire preuve de davantage de discipline
3) Je soutiendrais volontiers l'introduction d'un service militaire obligatoire
4) Je suis plus exigeant que la plupart des gens à propos de ce qui est bien ou mal
5) La police devrait avoir le droit d'écouter des appels téléphoniques privés lorsqu'elle enquête sur un crime
6) Les personnes au pouvoir ne divulguent pas d'informations sur les choses qui sont nuisibles pour nous
7) Un des problèmes avec les gens est qu'ils défient l'autorité trop souvent
8) Il est important de préserver nos coutumes et héritages
9) Je pense qu'il est important de faire perdurer les traditions familiales
10) Dans mon ménage, les membres de la famille ont leurs propres endroits autour de la table pour dîner
11) Je trie toujours les vêtements dans des catégories séparées avant le lavage
12) J'estime les routines régulières comme étant le plus important
13) Je pense qu'il est important d'être ponctuel
14) Ma planification des repas n'est pas due au hasard
15) J'aime étudier soigneusement les risques de financier pour ne pas qu'ils surviennent

B- Égalitariste

1) Si les citoyens de ce pays étaient traités de manière plus équitable, nous aurions moins de problèmes
2) Le gouvernement devrait veiller à ce que chacun ait un bon niveau de vie
3) Ceux qui sortent du lot devraient être taxés davantage afin d'aider ceux qui sont moins privilégiés
4) Le monde pourrait être un endroit plus paisible si sa richesse a été répartie plus également parmi des nations
5) La sécurité sociale est une contrainte pour les gens qui essai de gagner davantage pou réussir
6) La discrimination raciale est un problème très sérieux de notre société.
7) Ce dont ont besoins les nations est « une révolution de justice » pour une distribution plus égale des biens (marchandises)

8) La plupart des repas que je mange sont végétariens.
9) Je préfère des produits alimentaires simples et non traités.

C- Individualiste

1) Dans un système équitable, les individus les plus compétents devraient gagner davantage
2) Une société libre ne peut exister qu'en donnant la possibilité aux entreprises de prospérer
3) Si une personne peut acquérir des richesses, elle devrait avoir le droit d'en profiter
4) C'est juste que la vie ait tendance à trier ceux qui font un effort plus important de ceux qui n'en font pas
5) La croissance économique continue est la réponse à l'amélioration de la qualité de la vie
6) Ce pays serait mieux loti si nous ne nous inquiétions pas au sujte de l'égalité entre les individus
7) Gagner de l'argent est la raison principale au travail acharné
8) Je ne rejoins pas les clubs d'aucune sorte
9) J'ai tendance à être sceptique au sujet des principes d'alimentation saine

D- Fataliste

1) Cela ne sert à rien d'agir pour autrui, à long termes cela nous retombre dessus
2) La coopération avec les autres fonctionne rarement
3) L'avenir est trop incertain pour que l'on puisse faire des projets sérieux
4) J'ai souvent été traité de manière inéquitable
5) Un individu s'en sortira mieux s'il ne fait confiance à personne
6) Je ne me soucie pas de politique car je ne peux pas vraiment influencer les choses
7) La plupart des personnes se font des amis seulement parce qu'ils sont utiles pour eux-même
8) J'estime que la vie ressemble à une loterie
9) Même si vous travaillez dur vous ne savez jamais si cela vous aidera à obtenir le succès
10) Il me semble que quiconque vous voteriez les choses seront à peu près les mêmes.
11) J'ai peu d'investissements financiers.

Guide d'entretien et sources des questions

Rappel du contexte de l'entrevue : L'objet de ma recherche est de comprendre la façon dont a été décidée la sécurité de l'information, sur quels éléments elle a été pensée. Si nous faisons le pont entre votre décision et sa déclinaison « opérationnelle », je m'intéresse spécifiquement à la réflexion que vous avez initiée et conduite pour décider qu'il fallait protéger vote SI.

1. Profil de l'entreprise

- Quel est le secteur d'activité de l'entreprise vos avantages concurrentiels et vos spécificités ?
- Quel est l'effectif de votre structure ?
- Est-elle soumise à des réglementations particulières (telles que par exemple RGPD, CNIL, Données de santé…) *(influences externes isomorphisme coercitif, Williams et al. 2009)*
- Quelle est l'importance du SI en regard de vos activités, de la création de valeur de votre entreprise ? *(distinction entre SI comme support technique et SI comme support stratégique, Bandyopadhyay et al. 1999)*

2. Profil du dirigeant

- Quelle est votre formation ?
- Quels postes avez-vous occupés avant celui-ci ?
- Quelles expériences avez-vous acquises sur la sécurité du SI dans les postes précédents ? Avez-vous rencontrez, dans vos postes précédents des dysfonctionnements du SI ? *(risques vécus et risques connus, Slovic et al. 1979, Choobineh et al. 2007)*

3. Rôle du dirigeant

- Quelle est votre fonction au sein de l'entreprise ? Quelles sont vos missions ?
- Quel est votre rôle en tant que dirigeant ?
- Pour vous, qu'est-ce que la SSI ? *(Solms 2006 p. 167 établit les bases du MSSI sur « l'engagement du board et du top management)*

- Pour votre secteur d'activité quelle est l'importance de la SSI *(la SSI est principalement une question de gestion et d'affaires, donc les directeurs devraient être conscients de son importance, Soomro et al. 2016)*
- Pour vous quelle est la place de la SSI dans votre organisation ? *(principalement une question de gestion et d'affaires, donc les directeurs devraient être conscients de son importance, Soomro et al. 2016)*
- Êtes-vous concernés par les risques qui peuvent impacter votre SI ? Si oui, pour quelles raisons ? *(la responsabilité vis-à-vis du risque, Cadet et Kouabénan 2005 ; une responsabilité de direction générale, Solms et Solms 2006b, et la responsabilité pour le dirigeant lui-même, Moulton et Coles 2003).*
- Par qui les décisions relatives à la SSI sont prises ? (spécialistes internes ou le dirigeant, les deux, d'autres) ? Pourquoi, pourquoi ces acteurs ? *(La SSI comme une responsabilité de direction générale, Hu et al. 2007)*

4. Éléments considérés lors de la décision

- Comment cela s'est-il passé, c'est-à-dire comment avez-vous commencé à réfléchir à la SSI, comment des choses ont-elles émergé à propos de la SSI dans votre entreprise ?

OU

- Quand avez-vous pris la décision d'engager (analyser) la SSI ? Pour quelle raison avez avez-vous protégé votre SI ? Comment cela s'est passé ?

- À ce moment-là : (**risque / isomorphisme**)
    - De **quels risques SI** avez-vous voulu vous prémunir ? Comment ces risques pouvaient se traduire pour votre entreprise, quelles conséquences auraient-ils eu selon vous ?
    - Avez-vous rencontré des situations défavorables sur votre SI ? (Ou) Avez-vous vécu des situations particulières ou défavorables, ou des évènements qui ont marqués votre SI ?
    - Si oui, lesquelles ? Comment ont elle touché votre activité ? De quelle nature ont été ces **conséquences** (impacts d'image, financier, économiques, juridiques…) ?
    - Est-ce que des collaborateurs **internes vous ont alerté** sur les risques potentiels auxquels vous étiez exposés ? Lesquels ? Comment les avez-vous considérés (probable, illusion, non concerné… ?)

- Un dysfonctionnement a été évité et les conséquences potentielles que vous avez imaginées ou qui vous ont été indiquées ont alimenté votre réflexion ? Quelle est la nature de ces conséquences ? De quelle nature auraient-elles été (image, financier, économiques, juridiques…) ?
- Un événement particulier est-il survenu chez un de vos partenaires, fournisseurs, concurrents, qui vous a alerté sur les conséquences potentielles pour votre propre entreprise ? Quel a été cet évènement ? Quelles sont selon vous les conséquences survenues ?
- Votre entourage ou la presse vous ont informé du potentiel risque qui pèse sur les SI des entreprises ? Si oui lequel ou lesquels ?
- Une association ou un réseau professionnel dont vous ou votre entreprise êtes membre préconise de se prémunir des risques SI ?
- Un de vos partenaires, fournisseurs ou concurrents a-t-il mis en œuvre la SSI pour son entreprise avant ? Si oui, pour quelle(s) raison(s) pensez-vous qu'il l'a fait ?
- Des exigences réglementaires ou législatives vous ont été imposées, se traduisant par la mise en œuvre de la SSI ? Quelles ont été ces exigences ? Si vous y avez répondu, pour quelle raison ?

5. Renseignements pris sur les risques et la SSI

- Comment vous êtes-vous renseigné sur la SSI ? Quelles sources avez-vous utilisées et pourquoi ? Pouvez-vous donner un exemple ?
- Quels renseignements vous ont été utiles pour vous décider ? Pourquoi ces renseignements-là ?
- Comment ces renseignements ont influencé votre connaissance de la SSI ?
- Est-ce que ces renseignements vous ont informés sur les risques que vous perceviez ? Lesquels ? De quelle façon ces renseignements ont éclairé vos risques ?
- Est-ce que la prise de renseignement sur la SSI vous a permis d'identifier d'autres risques que ceux imaginés initialement ? Lesquels et pourquoi ? Pour quelles conséquences sur le SI ou vos activités ?

6. Validation (symbolique) de la SSI pour couvrir les besoins

- Après avoir pris ces renseignements, comment avez-vous projeté / imaginé la SSI qui vous conviendrait ? Comment avez-vous su qu'elle répondait à vos risques (si risque) /vos besoins (si règlement ou externe) ?
- Quels risques avez-vous alors projeté de couvrir par la mise en œuvre de la SSI ? Est-ce les mêmes que ceux qui ont été effectivement couverts lorsque vous avez mis en place la SSI « opérationnelle » ?
- Quels sont les apports que vous avez perçus pour vous et votre entreprise lorsque vous pensiez vous engager dans la SSI ?

Pour aller plus loin…

7. Organisation de la sécurité

- En synthèse, quels sont les éléments qui vous ont permis de dire qu'il s'agissait d'un besoin qui devait être satisfait, sans considérer les contraintes liées à sa mise en œuvre ?
- **SI** les compétences SI sont décrites : Pensez-vous que vos compétences sur le SI vous ont aidé à percevoir les risques ?
- Quelles sont vos préoccupations en termes de SSI aujourd'hui ? Et si cela a évolué, demander « pourquoi ces évolutions » ?
- Avez-vous revus les risques que vous souhaitiez initialement couvrir ? Si oui, pourquoi ? Comment avez-vous fait pour les revoir ?
- Diriez-vous que les risques que vous aviez décidé de couvrir sont les mêmes aujourd'hui qu'au moment de votre décision ? Si non, lesquels sont différents ?
- Par quelle(s) mesure(s) concrète(s) s'est traduite votre décision (exemple tel que :
    - Mise en place d'une organisation
    - Mise en place de règles
    - Délégation de cette problématique à vos collaborateurs
    - Appel à des prestataires externes)

Monographie des entreprises des dirigeants interviewés

E1 est « un cabinet de recrutement dont la prestation est dédiée aux cabinets d'expertise comptable et d'audit / commissariat aux comptes. Nous ne pourvoyons pas de missions d'intérim et travaillons uniquement sur des missions en CDI ou en CDD. Vous retrouverez sur ce site toutes les informations nécessaires à vos démarches : le fonctionnement de Filigrane, les métiers pour lesquels nous recrutons, nos coordonnées, nos études de rémunération, nos offres d'emploi… Que vous soyez candidat ou employeur, ce site vous est dédié. »

Tranche d'âge du dirigeant 30-35 ans, diplômé d'un BTS technico-commercial et d'une licence et master professionnel en science de l'éducation, a exercé dans un grand groupe dont l'activité relève de la gestion des ressources humaines et du recrutement.

3 personnes, CA 120 K€.

E2 est une agence **spécialisée en communication et marketing expérientiels**, « Nous concevons des aventures créatives qui favorisent la mémorisation des messages et des valeurs d'une marque. Nos expériences offrent du sens, de l'émotion et des souvenirs à partager ! Conseil en communication et production de solutions de marketing opérationnel. Nous concevons des dispositifs de communication décalés pour les entreprises, institutions ou professionnels. Ils offrent des expériences sociales créatives et ludiques qui répondent aux besoins d'émotions à partager. Que la Marque soit commerciale, employeur ou territoriale, nos scenarii donnent vie à son discours en créant une mémoire commune durable. »

Tranche d'âge du dirigeant 30-35 ans, diplômé d'un BTS domotique, d'une École de Commerce (Kedge) avec une spécialité Commerce International, apprentissage dans le secteur de l'industrie aéronautique, avec une compétence marketing-intelligence économique.

3 personnes, CA 200 K€

E3 est « spécialisée depuis plus de 40 ans dans l'ensemble des solutions d'éclairage public. Nous proposons des alternatives pertinentes et durables dans le secteur de l'éclairage à économies d'énergie afin de répondre aux évolutions environnementales et technologiques. Notre crédo l'éclairage éco-logique »

Tranche d'âge du dirigeant 45-50 ans, diplômé d'un bac-pro comptabilité précédemment professeur de tennis durant 18 ans.

CA 1,2M€ 5 personnes

E4 est « une TPE créée depuis maintenant 1 an et on est fabricants de bijoux, principalement vendeurs sur le Web et un petit peu sur des étals mais l'essentiel est sur notre « shop » que nous avons développée sur le Web. »

Tranche d'âge du dirigeant 40-45 ans, diplômé de l'Ecole Supérieure de Commerce de Compiègne a principalement œuvré dans des postes de direction générale, communication et publicité

CA inconnu, 3 personnes

E5 société de courtage en assurance, créée en 2001, pour un « accompagnement efficace et modulable en fonction de votre situation, pour vous informer et pour vous suivre au cas par cas dans vos projets de souscription à une mutuelle d'assurances. Au service des particuliers et des indépendants, nous accompagnons également les entreprises. Nous vous proposons des solutions objectives et impartiales en ce qui concerne le prêt de mutuelle de prévoyance santé, la retraite, l'épargne et le placement. »

Tranche d'âge du dirigeant 50-85 ans, maîtrise en droit des affaires option fiscale à l'université, DESS droit des assurances et un Master 2 de gestion du patrimoine. A occupé un poste de contrôleur pour une société d'assurance durant 15 ans.

CA de 300K€, 1200 clients, 2 personnes, profession réglementée dépendante de l'ACPR, utilisation de données médicales

E6 est une société de **créateur de teintes et matières**, … qui fabrique chaux, bétons cirés, peintures, enduits décoratifs et métallisation et accompagne ses clients dans les réalisations en résidentiel et lieux publics.

CA inconnu, 25 personnes

E7 est une **société d'expertise comptable** : « Un expert-comptable n'est pas seulement un homme ou une femme qui s'occupe de la comptabilité des entités, il aide aussi ses clients à gérer et sécuriser son entreprise et à mener à bien ses projets »

Tranche d'âge du dirigeant 45-50, Diplôme d'études supérieures commerciales, administratives et financières

CA 1M€, 20 personnes, 4 sites, Profession réglementée,

E8 est une société de biscuiterie, confiserie, chocolaterie dans des réseaux de franchise et des boutiques en propre. « Avec des clients qui sont, pour 30 ou 40% du CA aujourd'hui, des particuliers, sur nos boutiques en propre et après évidemment des franchisés qui sont des clients pros et après il y a plein de secteurs d'activités connexes : cadeaux d'affaires, tourisme d'affaires, on travaille avec des hôtels, des épiceries fines, etc… mais ça reste des secteurs vraiment connexes. »

Tranche d'âge du dirigeant 45-50, autodidacte

CA 2M€, 12 personnes sur 4 sites

E9 est une **société d'expertise comptable** qui consiste elle-même en 2 métiers :

- La production des comptes de nos clients, c'est-à-dire l'établissement des déclarations annuelles : obligations du Code du commerce, obligations fiscales et obligations du Droit des Sociétés de publications, l'activité sociale issue des bulletins de paie qui est un corollaire de cette mission.
- L'autre activité c'est l'activité de conseil c'est-à-dire d'assistance et de suivi du client dans le but d'amélioration de ses performances

Tranche d'âge du dirigeant 50-55, DESS finances, DU Gestion du patrimoine

CA 600K€ 4 personnes Profession réglementée

E10 est une société spécialisée en épidémiologie, en pharmaco-épidémiologie et dans les interventions en santé publique et numérique. Elle offre une expertise avérée tant au niveau national qu'international et des prestations full services. La diversité des savoirs regroupés en son sein garantit la maîtrise des projets, de l'idée à la publication.

Dès sa création E10 a misé sur le facteur humain afin de constituer une équipe polyvalente à haut niveau de performance.

Tranche d'âge du dirigeant 40-45, DEA en ingénierie des organisations et un doctorat en science en sciences économiques

CA 95M€, 1000 salariés, 400 sous-traitants

E11 propose des solutions pour traiter les appels téléphoniques de clients, patients ou usagers. Elle dispose de plusieurs offres d'externalisation de standard téléphonique de la pris en charge des appels sont sur ses plateformes téléphoniques avec tout le professionnalisme de nos opérateurs au secrétariat. Elle se distingue par des outils télécom qui permettent de gérer simultanément des milliers d'appels en temps réel l'appui de CRM et de technologie totalement redondante où les données sont sécurisées.

Tranche d'âge du dirigeant 50-55, Doctorat de physique, École Normale Supérieure

CA inconnu, 15 salariés

E12 est une société créée en 2010, « en pleine croissance qui entre 2016 et 2017 a fait 30% de CA en plus » et qui travaille sur le big data pour l'industrie du tourisme avec une solution historique qui est le benchmarker soit une veille concurrentielle qui va récupérer des prix sur Internet des prix de tourisme, du voyage au camping en passant par les locations de ski et le ferry . On récupère des données qui proviennent du Web en XML par du scraping.

Tranche d'âge du dirigeant 35-40, MBA spécialisé Luxury brand marketing and international management

CA inconnu, 8 personnes

E13 est une agence immobilière dont l'activité repose sur la transaction et la gestion locative. Le rôle du dirigeant est de gérer cette entreprise notamment « pour dynamiser les équipes les accompagner sur le terrain et de valider les évaluations »

Tranche d'âge du dirigeant 35-40 ans, diplômé d'un BEP comptabilité, d'un bac pro vente - représentation et d'un BTS professions immobilières

CA 350 K€, effectif de 8 personnes

E14 Entreprise familiale artisanale qui opère dans le secteur du paysage c'est-à-dire création et entretien de jardins et tout ce qui est annexe autour du jardin. « La garantie qualité pour vos espaces verts. »

Tranche d'âge du dirigeant 60-65 ans, autodidacte

CA inconnu, 12 salariés

E15 a une activité de gestion hôtelière, 25 chambres à Toulon, une partie des réservations est établie par avec Booking.com.

Tranche d'âge du dirigeant 55-60 ans, autodidacte

CA inconnu, 5 salariés

E16 est une société qui propose des formations professionnelles courtes (quelques jours) et longues (une année) en alternance auprès d'un public de professionnels en poste en entreprise.

Tranche d'âge du dirigeant 55-60 ans, diplômé d'une licence « en commercial »

CA 400 K€, 4 salariés

E17 est une société du secteur « événementiel et étudee » (marché, publics, analyse financière, …)

Tranche d'âge du dirigeant 55-60 ans, diplômé d'une licence « en commercial »

CA inconnu, 8 salarié Dirigeant interrogé : 50ans (environ), son entreprise emploie 8

Entretien avec D11

L'idée est de préciser avec vous ce qui s'est passé lorsque la décision de protéger le SI a été prise. Avant de rentrer dans le vif du sujet, j'aurais besoin de savoir quelle est votre activité, votre formation, quels postes vous avez occupés précédemment, quelle est votre responsabilité en tant que dirigeant ?

Le groupe c'est à la fois une SSII qui est éditeur et opérateur de solution informatique et télécom en direction des entreprises au sens large et je dirais aujourd'hui précisément les centres d'appels. Dans ce groupe il y a aussi un centre d'appels qui est spécialisé on va dire dans la validation des dossiers de gros comptes et de la même manière sur les dossiers spécifiques ou la sécurité notamment est importante par exemple des hôpitaux des entreprises de la défense donc forcément on a les spécificités un petit peu particulières avec eux du fait qu'on peut éventuellement travailler sur un système d'information ou intégrer des informations de leur part voilà pour le Groupe général.

Moi au sein de ce groupe, à part la direction générale j'ai la direction des opérations donc autrement dit tout ce qui est dans la gestion du système d'information au sens large du système de télécommunications au sein de la filiale et globalement la responsabilité au sein du groupe que le dossier soit bien traité. Donc des fois vous avez des clients qui peuvent m'avoir un accès direct à moi pour des dossiers très très sensible ou des problématiques sensibles au sein de l'entreprise on a la partie qualité qui et gérer essentiellement au niveau du groupe par un responsable qualité qui est là surtout pour valider que le livrables qu'on fournit à nos clients

Au niveau du groupe on a des opérateurs tout ce qui a de plus classique qui utilisent un ordinateur et télécom de base en se connectant sur une application Web pour la partie SI et un système IP Centex pour la partie télécom ce qui signifie que par exemple ils peuvent très bien sur le petit plateau ici ou de chez eux, ce qu'ils font éventuellement le samedi plutôt que de venir ici ou voir même quand on travaille avec des gros dossier et de fort volume comme par exemple le « poseur de pare-brise » on a vraiment des quantités d'appels très importantes parce que eux-mêmes travaillent avec un système de distribution et ont des appels et des commandes et donc leurs appels arrivent tous chez nous dans notre groupement en tant qu'opérateur c'est comme si ça tombe sur notre réseau et distribue ensuite à l'opérateur disponible qui se trouve en France ça c'est la partie Groupe.

Donc moi je suis en charge que tout se passe bien au niveau de la gestion des projets et l'autre filiale est un responsable de la sécurité des SI et télécom pour l'ensemble du groupe et pour nos réseaux et il partage tous notre système d'information et de télécommunications ça c'est très important.

La partie du SI qui est en rapport avec les contrats, les factures, les devis et tout cette partie-là est gérée à travers un super CRM sur le Web qui permet de gérer tout le cycle de vente pour éventuellement la partie dénonciation de contrat, plainte tout, le courrier officiel, pour le coup c'est principalement Outlook, sachant qu'on s'en sert comme base de donnée ainsi tous les responsables de portefeuille ont dans leur Outlook un dossier par client avec tous les éléments de discussion avec ce client est archivé dans notre système.

Donc ça c'est la partie du SI en qui gère tout ce qui est commercial et tout est sur ce type de système en terme de sécurité nous on a fait le choix même si on propose du Cloud finalement nous on est plutôt du style à vouloir tout posséder en interne enfin pas posséder les licences, mais qu'on puisse tout gérer de A à Z.

Notre principe est de tout développer en interne et d'avoir la maîtrise de tous les systèmes ça vraiment quand j'ai monté l'entreprise c'était mon souhait premier.

Donc dans le cas de super CRM il est installé dans un de nos Data Center qui sont et pour le coup contrôle toute la sécurité pour y accéder donc typiquement on a fait un style de réseau privé qui nous permet d'ici ou de certains points spécifiques d'accéder à ce CRM, ce qui nous garantit éventuellement une certaine confidentialité des données ne serait-ce que par rapport à un collaborateur qui est de l'extérieur qui pourrait accéder à ses données aller récupérer sur CRM avec ses propres login password par exemple, ce qu'il pourrait très bien se faire si on était dans une utilisation pure Cloud comme le propose par exemple super CRM ou n'importe qui pourrait éventuellement se connecter dessus en ayant déjà aussi login password. Donc cela nous permet et par ailleurs on a déjà eu des soucis à un moment avec cette société et c'est vrai que la menace de nous « couper les données » n'a pu être portée du fait que les données étaient chez nous…

Donc l'idée c'est vraiment de pouvoir, du fait que ce soit dans nos propres baies sur des serveurs dédiés au sein d'un DC, quels que soient les services qu'on peut proposer à nos clients c'est toujours avoir la maîtrise de ce qu'on peut soit utiliser soit proposer tant sur le logiciel que sur la partie donnée.

Tout le développement de nos propres suites de notre écosystème, logiciel au sens large et voix sur IP. Dans une approche sécurité et sûret, et pour la sûreté de fonctionnement on a à la fois mis des PRA et tout un tas de système de reprise d'activité après un crash. Comme on a changé de bureau on a réfléchi à aller même jusqu'à disposer de l'appartement qui comprend nos anciens bureaux sur une plus petite surface mais qui nous permettrait d'être en mode dégradé et d'avoir très facilement accès et de laisser en place le réseau avec la possibilité d'accéder au Cloud, il suffit de prendre son écran et son téléphone et de prendre chacun son portable ce qui est un plus pour les opérateurs et du coup en une heure en deux heures on est de nouveaux en pleine action sans difficulté particulière, si il y a un incendie on aurait des délais extrêmement courts. Malgré le coup, il faut quand même garder l'appartement mais c'est quand même quelque chose auquel je réfléchis vraiment parce qu'on va se diriger vers le domaine de santé et c'est un petit plus qui sera peut-être qui sera important à garder donc là il y a les postes dedans les câbles et ça repartira immédiatement…

Donc je disais on est que sur les serveurs dédiée avec toutes les redondances sur la machine elle-même ensuite à partir de la machine on a la possibilité sur la partie logiciel que sa partie base de données, on est multi DC donc on gère les accès de nos clients à travers un portail ainsi que toute l'architecture est en place depuis 2001 c'est-à-dire que quand un client se connecte il est redirigé vers les ressources disponibles qui puisse se trouver sur différents DC ce qui fait que si jamais il y a un problème électrique ce qui arrive de temps entends sur le data Center ou des chose comme ça, on a vu régulièrement des petits soucis, il va être dispatché automatiquement ou semi automatiquement vers d'autres ressources et de la même manière la base de donnée étant circulaire permet la réplication donc si un pépin sur une base de donnée et qu'elle devait devenir indisponible là aussi avec des opérateurs différents et des opérateurs télécoms différents et indépendant les uns des autres on est arrivé à avoir une disponibilité dans le service qui est très importante…

Avant de prolonger votre présentation, pouvez-vous m'en dire plus sur votre profil ?

Je viens de l'école normale supérieure et j'ai fait des études très théorique dans le domaine de la fusion thermonucléaire après normal je suis parti sur Oxford pour

travailler à côté sur le JET qui est en fait à un TOCAMAC dans le domaine de la fusion thermonucléaire c'est un peu le projet ITER en beaucoup plus petit de celui de Cadarache et c'était le plus gros acteurs à l'époque et ensuite je suis parti à l'EPFL où là j'ai fait de la recherche fondamentale et entre-temps j'étais fonctionnaire au niveau européen

J'avais aussi un projet de monter une entreprise est en 2001 c'était l'occasion et donc j'ai lancé l'entreprise comme ça sans étudier le marché et pour le coup vraiment avec un profil de théoricien très très loin du client. C'est plutôt ce parcours au départ en 2001 on a tout de suite travailler dans le « Cloud » parce que finalement les grandes entreprises dans lesquelles j'étais travaillé déjà dans un Cloud privés et c'était un peu ça on travaillait tous avec des postes déportés sur le serveur distant et moi-même j'avais travaillé sur le Grid et c'est tout ça que j'ai mis en place pour la société et notamment cet architecture qu'on utilise toujours, architecture multimodale avec une grande disponibilité du service extrêmement importante et cette facilité de mise à jour des versions pour nos clients qui sont sur deux versions différentes, on a des systèmes de management de mises à jour automatique de ces version sur l'ensemble, donc il y a toute une réflexion qui a déjà été menée à cette époque…

Dans les précédents postes vous avez acquis des expériences par rapport au SI

Oui j'étais dans la partie informatique enfin quand on fait la physique on fait beaucoup de théorie et de modélisation tout passe par des gros calculateurs les fameux « grid » et ensuite en tant que chercheur même si on peut avoir le support de techniciens informatiques, on doit être capable de maîtriser les capacités pour faire du calcul en parallèle sur plusieurs machines... donc c'est à la fois l'avantage et les reproches qu'on peut faire à un chercheur, c'est qu'il se doit d'être autonome

Avant 2001 avait déjà vous avez-vous déjà rencontré des situations défavorable sur votre Si?

Non pas vraiment à cause de crash ou de problème de sécurité et la disponibilité oui on avait des temps de calcul qui valait une fortune donc c'était la lutte pour avoir droit aux expériences ces journée ou demi-journée d'expérience et calculateur donc c'était plus ta disponibilité.

À partir de 2001, création de votre société sur la base de la grille ?

C'est sur cette approche de Grid avec les premiers data Center dans lequel j'ai mis des serveurs c'était une maison vers « l'étang » il y avait juste une liaison spécialisée avec Orange c'était assez folklorique il y avait même pas encore du débit Internet à 400k donc moi-même quand je devais faire des démonstrations je venais avec un serveur où j'avais mon système sur le serveur et les clients avaient très peu Internet avec des modem en 56k, donc bon c'était une autre époque, mais dès cette époque-là on s'est installé sur ce créneau on avait la vision ce que l'Internet c'était pas juste faire des petits sites Internet voir juste une vitrine rien d'autre et qu'on pouvait vraiment faire des applications et c'est cette approche applicative qui dès le départ m'a séduit et dans laquelle je me suis lancé…

En 2001, quelle était l'importance de la sécurité de ce système informations pour vous ?

Elle était surtout centrée sur la sureté de fonctionnement, la disponibilité en fait que le service soit toujours accessible pour les centres d'appels. Si jamais on coupe le téléphone vient à rencontrer un dysfonctionnement les personnes sont immédiatement au chômage technique ! Donc on est vraiment sur des thématiques où la disponibilité du service est essentielle, donc dès le départ il fallait trouver une solution qui nous permette de rendre le plus sécurisé possible l'accès à la ressource et l'autre chose qui était aussi très importante c'est que nous on rentrait sur un marché qui existait déjà et les concurrents en fait se déplaçaient de centre d'appels en centre d'appel, faisaient les installations aussi quand il y avait un problème sur le serveur et quand il y avait un incident il devait prendre l'avion ils étaient à Lille à l'époque ça avait des coups important et des délais importants.

Donc l'idée pour nous c'était évidemment d'arriver à faire une proposition de service plus en adéquation avec les postes parce que finalement même si au début, les deux premières années, on se déplaçait parce que les accès Internet était plutôt rare chez les clients mais une fois que ça s'est démocratisé et bien là on faisait des démonstrations à distance et ensuite on envoyait les Cisco par la poste il branchait le routeur et on installait à distance ce qui était une vraie facilité pour le client. Donc ça c'était assez intéressant…

Vous utilisez souvent le pronom « on ». Vous avez une vision partagée sur ces sujets ?

J'ai dit « on » parce qu' aujourd'hui je suis très équipe mais à l'époque non j'étais tout seul et faire vivre l'entreprise parce que quand on est éditeur il faut construire donc la société a du émerger du fait que j'ai des contacts avec des grands comptes où j'intervenez comme consultant et ensuite quand j'ai eu mon premier salarié on faisait du développement donc très éloigné de ce qu'on fait aujourd'hui…

Mais finalement d'où vient cette compétence sur la sécurité des systèmes informations ?

Quand on a m s en place la grille dans ma précédente entreprise, c'était de la pure R&D. Quand on en vient à discuter dans différents groupes de ce sujet, c'est souvent ce que je dis, c'est tout l'intérêt de faire une thèse ! En fait moi je pense que cette capacité que j'ai eu à voir tout ça, ne vient pas forcément de normal Sup, mais vraiment cette capacité à apprendre à réfléchir à se remettre en question sur des choses nouvelles je l'ai vraiment acquise pendant ma thèse.. Après une fois que je fais la thèse j'ai continue à faire des recherches, mais c'est là que j'ai appris à réfléchir par moi-même sur des choses nouvelles parce qu'avant ça j'étais vraiment en recherche fondamentale …

Entre 2000 et 2004 avez-vous eu autour de vous des gens qui se sont retrouvés dans l'impossibilité d'assurer à la disponibilité de leur service

En fait non personne parce qu'on était les premiers sur le secteur… Les autres ils n'arrivaient pas vraiment, le marché existait pas vraiment j'étais sur les solutions locales même certains étaient encore avec des fenêtres DOS ça avec un applicatif installé sur un serveur local ou voir même sur les PC … et c'est finalement assez tard ou on a eu nos premiers concurrents sur le Web un peu je veux qu'après avoir mis en place cette architecture…

Donc on va partir de 2001 en dehors de la disponibilité à quelles autres risque vous avez pensé ?

Bah il y a des risques d'intrusion sur le serveur… Quand on parle de disponibilité c'est déjà très largement vraiment tout ce qui est risque machine, risque dans les DC, les accès électriques, des accès Web multifournisseurs pour nos propres client,

histoire éventuellement d'avoir des zones d'échanges en inters-opérateur différentes toutes cette partie avec la **redondance** qui est vraiment très importante ensuite ça à la fois logiciel et Telecom il y a quand même un spof c'est quand même le numéro de téléphone qui est lui est un peu comme une adresse IP doit être référencé à l'endroit et s'il a un problème on peut pas faire grand-chose… mais sinon tout le reste peut être sécurisé

En cas d'attaque externes à l'entreprise où là pour le coup, même si parfois c'est assez pénible, de l'ordre par exemple d'un déménagement on a oublié certaines choses on avait plus d'accès et donc c'est un petit peu compliqué mais effectivement on a notre propre sécurité avec des FW qui permettent de bien contrôler les accès que ce soit même sur certains on peut pas y accéder en acheter des terres en dehors de notre réseau privé on est pas en VPN, on pourrait l'être aujourd'hui mais c'est juste que par rapport à notre réflexion, on pourrait peut-être franchir une étape avec VM Ware on peut bien sûr actualisé entre guillemets les routeurs et surtout créer finalement des VPN.

Donc on a été amenés à faire ça pour des demandes de l'hôpital et on était assez loin pour pouvoir travailler pour que des différents collaborateurs dans différents points de France puisse travailler sur un même site à travers justement un nœud NSX qui nous permettait de pouvoir gérer ces accès en VPN . Donc c'est vrai qu'on pourrait aller dans cette direction on l'a pas fait, je suis pas sûr qu'aujourd'hui on le fasse par rapport à nos priorités… il faut y réfléchir parce qu'évidemment ça amène des contraintes complémentaires pour chacun pour travailler puisque dans le cas d'un FW c'est très simple de changer des règles pour pouvoir éventuellement faire qu'un équipe particulière puisse travailler avec des free-lance pour des développements pour nous et là on doit faire des configurations de FW spécifiques

Donc au début on était sur des considérations très basiques fournies avec la machine et puis aujourd'hui on a notre propre configuration assez aboutie pour me sécuriser sur la partie logicielle et encore plus sur la partie télécom pour le risque qui est colossale parce que beaucoup de boîte ont coulé à cause de ça : nos amis israéliens d'ailleurs et russes sont les pires parce qu'ils s'amusent à casser attaquant pour le CIP, c'est un protocole qui est un peu faible, ils attaquent les machines pour prendre le contrôle d'un compte, et le grand jeu c'est dans ce cas-là de revendre les minutes communications que ce soit pas le satellite limite ou sur des pays où c'est assez cher, etc et là vous vous retrouvez avec une note que vous allez devoir régler et qui peut

être de 200 ou 300 000 € en une nuit, c'est énorme ! Donc là pour le coup effectivement la partie sécurité dans ces systèmes est fondamentale notamment dans la gestion le protocole le choix les protocoles n'est pas un en CIP, en MGCP, c'était pour essayer d'être le plus sécurisé surtout sur la partie télécom pour là c'était vraiment important…

Pour les données, c'est un peu différent parce que les attaques externes nécessitent de passer les frontaux donc plus compliqué….

Quelles sont les raisons qui vous conduisent à mettre l'accent sur les attaques externes ?

Oui entre autre mais aujourd'hui c'est même dans notre réflexion actuelle c'est les attaques internes… Il y a eu un collaborateur qui récupère des données, on a eu le cas d'un commercial il y a huit ans c'est rare évidemment, sinon c'est compliqué d'avoir une équipe, on s'est rendu compte que ce commercial travaillait dans notre dos et pouvait même reprendre des propositions à son compte et les refaisait à d'autres clients moins chères, avec récupération de clients après donc ça c'est un premier. D'où effectivement dans l'usage du CRM on a mis quelque procédures pour pouvoir empêcher ce genre de choses et qu'on a pu généraliser dans nos propre système informations pour nos propres clients à savoir qu'on peut pas exporter comme ça une base donnée client chez nous ou patient ou ce qu'on veut un opérateur ne veut pas le faire comme ça même nos propre clients ne peuvent pas le faire comme ça pour pouvoir le faire ensuite dans un fichier Excel et le revendre comme il veut

C'est ce qui s'était passé avec la commerciale, récupérer des fichiers et travailler ses fichiers éventuellement des devis qu'il avait fait alors qu'elle avait pas pu le faire sur d'autre portefeuille et qu'il avait pas le droit pour y accéder mais par contre sur son propre portefeuille oui.

Donc c'est sûr que si on a l'accès depuis chez soi, l'intérêt est qu'on peut travailler à distance j'avoue que depuis le départ je suis pour la loi à la déconnexion donc une fois qu'on a terminé le travail on n'a pas à travailler en dehors des heures ouvrés et de ce fait là je n'ai pas de collaborateurs qui auraient besoin d'accéder au système d'information en dehors des heures. Finalement cela règle une partie de la problématique après aujourd'hui on a beaucoup d'opérateur qui travaillent depuis chez eux avec des accès particuliers mais c'est sur nos outils métier donc avec des accès qui sont contrôlés et verrouillés à ce niveau-là et n'ont pas la capacité

justement par exemple de récupérer les bases de données de nos clients ou des clients de clients ou pouvoir éventuellement faire quelque chose quoi…

Autre chose parce que là il y avait juste un danger entre guillemets économique, ou financier, comme je vous dis, ce n'est pas forcément pour nous le truc le plus important. Le point qui a été le plus important et qui m'a vraiment ennuyé c'était un de mes collaborateurs de l'informatique, un de mes ingénieur qui a un moment a commencé à faire vraiment des grosses grosses conneries, à saccagé une partie de nos codes sur le SVM à saccagé des éléments importants de notre informatique à vouloir même ouvrir parce qu'il avait aucune notion de la sécurité donc il utiliser des VPN privé depuis son poste pour pouvoir contourner notre FW interne etc… donc quelqu'un d'assez folklorique et malheureusement j'ai eu tort de reconduire sa période d'essai et du jour au lendemain c'est devenu une catastrophe ! bon on s'en est séparé mais n'empêche que là j'ai vu tout le risque et là on a vraiment perdu du temps pour tout remettre d'équerre et donc là ça a été vraiment pour moi une prise de conscience on m'en avait déjà parlé qu'aujourd'hui le risque est quand même finalement est beaucoup plus important en interne qu'en externe. En externe on a beaucoup d'outils pour ça mais en interne on se laisse parfois un peu aller comme les login sur les PC etc.. ou c'est souvent une catastrophe et chez nous ça l'est aussi d'où le fait qu'aujourd'hui je recherche une solution de contrôle d'accès unifié. Avec une gestion des droits affinés sur chaque PC. On a les mêmes problématiques avec les ingénieurs on leur donne des droits plus ou moins administrateur sur leur poste pour qu'ils puissent travailler et donc il y a des difficultés qu'il ne faut pas négliger ça aujourd'hui c'est le projet sécurité qui est chez nous et qui doit se faire dans les trois mois.

Après on a aucune donnée en local, pour nos clients, en local on a juste un serveur de fichiers qui sert pour notre documentation mais toutes les données stratégiques sont dans le cloud.

Je reviens sur les événements provoqué par votre ingénieur. Était-ce avant ou après le départ du commercial, n'était-ce pas une problématique « interne » ?

Oui mais sans avoir le même impact… si vous voulez l'attaque avec le commercial je l'ai classé comme une attaque « classique » : un commercial qui part avec son fichier clients, c'est classique dans le sens où ce sont des choses qui arrivent parce que je

connais d'autres entreprises à qui c'est arrivé. Moi dans le cas présent ça a été plus simple, comme ce sont des collaborateurs qui s'en sont rendus compte, on a fait une petite réunion c'était rapide et il a vite compris la problématique donc ça s'est vite arrêté. Et finalement le vol entre guillemets ou son action a duré quelques semaines en fait c'était très court donc il a rien pu en tirer réellement derrière…. Mais moi ça m'a juste fait pensé notamment à une boîte où un des commerciaux était parti avec leur fichier clients mais tous leurs fichiers clients et avait monté sa structure après… donc j'étais au courant parce qu'à l'époque c'étaient des potes qui avaient monté leur boit en même temps que moi, et cela leur avait fait un sacré coup, après ils ont attaqué et ils ont gagné et l'autre entreprise a disparu mais malgré tout ça leur a fait un sacré coup parce que finalement ils ont cassé les prix ça a été un vrai problème qui a bien perturbé leur business si vous voulez.

Et puis moi, ma mère a été comptable dans une entreprise et elle m'avait déjà parlé de ce genre de choses malheureusement que c'était des choses qui arrivaient et là il y a des limites dans la sécurité c'est que les informations que la personne manipule dans l'entreprise, elle-même y accède et les traient. Donc quelque part ce qu'il faut c'est qu'elle ne puisse pas partir avec tout le fichier mais son portefeuille seul, malheureusement on est un petit peu coincé. Alors bien sûr il y a des éléments qui permettent de les attaquer, on peut mettre certains éléments dans le contrat de travail et aussi parce qu'on accède à ces informations par le login et mot de passe justement quand on s'est rendu compte si on a pu régler le problème rapidement c'est parce qu'on avait tout à faisceau de preuves de ces accès illicites de son travail et de surcroît des enregistrements téléphoniques, parce que comme il ne pouvait pas travailler de l'extérieur sur son système il aurait pu au moins appeler avec son portable il a travaillé directement avec notre propre système de télécommunications et nous on a déclaré auprès de la CNIL le fait qu'on pouvait enregistrer les communications et dans le contrat travail est spécifié que ça peut faire partie de preuve avec tout un discours précis qui permet de pouvoir effectivement utiliser ces informations-là, à charge même si je vous avoue que c'était pas forcément dans cet esprit-là mais ça peut être par rapport à des comportements inadéquates vis-à-vis des clients et autre. Là ça nous a permis tout simplement de le convoquer il a réfuté mon accusation, je lui ai fait écouter l'enregistrement avec un de nos clients et il disait spécifiquement qu'il voulait monter son entreprise et récupérer des contrats avec une proposition de réduction alléchante pour ses futurs clients. Donc quand on a

ce genre de choses généralement ça suffit pour le collaborateur laisse tomber et aille agir ailleurs et c'est ce qui s'est passé. Nous derrière on pas eu de conséquences de ce fait là…

Pour le collaborateur informaticien, lui a une place beaucoup plus importante dans notre structure parce qu'il touche au cœur donc que c'était un recrutement pour qui je suis même passé par un chasseur de tête pour tout vous dire, une première fois où j'ai pris un chasseur de tête et je l'ai bien regretté… et donc c'est quelqu'un qui était censé être très expérimenté et qui été en fait était pas très bon et qui a très mal vécu le fait qu'il n'était pas au niveau et ça s'est très très mal passé… pas de remise en question, il avait l'impression qu'on considérait son travail comme pas correct, ce qui était un peu le cas et quand j'essayais de l'accompagner il bloquait et il nous a fait plein de cochonnerie jusqu'à, on s'en est rendu compte un peu plus tard, jusqu'à même expliquer à des commerciaux comment utiliser des VPN pour contourner notre fire-wall par exemple. Bon quand même plutôt lourd, et après du coup il a fallu expliquer pourquoi on a un fire-wall pourquoi il y a cette traçabilité, s'il y a un fire-wall et des règles c'est justement pour ne pas que vous les contourniez et intégrer tout ça en faut dans le contrat travail pour bien préciser à chacun qu'il faut respecter les règles parce que ces VPN sont vraiment problématiques parce que un fire-wall ne peut pas empêcher ce genre de contournement et d'usage…

Quelles autres expériences peuvent relever selon vous de l'attaque externe ?

Oui, en fait à un moment on a eu du captage de R&D. En fait une entreprise est devenue client et en devenant client ils ont pompé notre logiciel, ils se sont fait leur cahier des charges comme ça. Comme je vous le disais on ne se déplace pas chez le client, on livre, on donne les logins passwords donc ils ont monté une adresse bidon, parce que d'après ce que j'ai compris cela a duré quelques années, au final donc par une petite structure un petit machin et puis cela leur a permis de faire leur développement.

J'ai une autre idée de même ordre, c'est normal après 15 ans d'avoir plusieurs anecdotes ça on s'en est rendu compte par les clients qui nous ont dit qu'ils avaient eu une démonstration et qu'ils « ont ri parce qu'on a vu une phrase qu'on avait vu chez vous et quand j'ai (ils ont) posé la question ils ont pas pu me répondre » (rire)

alors que nous on peut répondre sur des mots qui sortent de l'ordinaire et qu'on a dans nos applications....

Après c'était pas une récupération de code source c'était finalement une copie par cahier des charges d'une application parce que dans nos métier une des fonctions de base c'est la gestion du planning pourquoi on prendrait pas Outlook et imaginerait pas des choses assez pertinentes, dans nos métier il y a plein d'aspect métier liés à des petites choses du fait qu'on délocalise l'accueil téléphonique pour la prise de rdv qui font la richesse de l'applicatif qui se construisent en interne et aussi avec nos clients.... et c'est cette richesse, cet actif qui fait l'intérêt de la solution et évidement quelqu'un qui débarque en nous copiant gagne toute cette expérience et gagne 5 ans.

Il y a un risque qui aujourd'hui je pense, est devenu vraiment important. Moi j'étais confronté en 2013 à quelque chose, pour moi de plutôt grave : c'est un de mes concurrents qui par l'intermédiaire d'un centre d'appels, qui était à un de nos clients d'ailleurs, en lui faisant une belle offre économique à ce qu'on a compris après coup, a obtenu une licence opérateur chez eux, ce qui leur a permis de faire un robot, qui à partir des logins passwords de comptes réels, donc avec lesquels ils étaient autorisés, sont venu pompé les données de nos applicatifs du compte client en question. De ce fait on a eu comme ça des migrations un peu sauvages, et même des choses un peu bizarre, c'est-à-dire qu'avec son propre service, son robot mettait à jours des données chez nous. Donc un sorte d'intrusion par ce biais-là, avec un login password adéquate mais pas par un humain, par un robot, quelque chose qui est illégal mais qui s'est pratiqué et qui d'ailleurs aujourd'hui encore nous pose question par rapport à la RGPD… là on est couvert parce que si c'est notre client qui fournit le login / password on peut pas faire grand-chose, sinon que c'est industrialisé du fait du robot il va scanner toutes les données possibles quand je vous dis qu'on peut pas faire l'export de base de données globale mais avec le robot on le fait tourner et on perd quand même finalement ces données qui sont sur le compte… On recherche une solution pour détecter / optimiser ce genre de chose, en complément des mesures basiques qu'on a déjà mise en place mais qui sont trop légères… Là ce sont des problématiques sur nos services de base, dès qu'on est sur des clients sensibles il y a du VPN avec des poules d'adresse IP fixe même certains gros clients ont des adresses IP dédiées avec des accès filtrés…

Justement par rapport à ce client grand compte hôpitaux et défense est-ce qu'il y a des demandes particulières ou des exigences de sécurité ?

Oui des demandes, notamment relatives à l'ANSSI et d'ailleurs je demande à mes techniciens de regarder leurs recommandations en terme de sécurité et de l'état de l'art pour se mettre à niveau de leurs connaissances. D'ailleurs les collaborateurs non informaticien, s'ils ont des questions sur la sécurité ou quoi que ce soit d'autre doivent venir voir les techniciens et leur poser toutes question.

En regard de ces systèmes et des mesures que vous avez mis en place, finalement quels sont les risques que vous avez couverts ?

La sûreté de fonctionnement... c'est plutôt dans le parcours d'une société qui se structure qui se développe qui a de plus en plus de moyens parce que soyons clairs, cela coute cher aussi donc aujourd'hui je sais pas si on va garder ce site de backup c'est en réflexion, notamment par rapport au budget annuel à peu près 15000 euros, ce qui n'est pas non plus hallucinant comme budget mais enfin bon a priori il servira à rien typiquement il y a peu de chance, enfin peu de chance… c'est le principe de l'assurance, j'espère bien qu'on aura pas d'incident, d'incendie dans nos bureaux mais c'est vrai que si ça devait arriver aujourd'hui, toute la réflexion est de savoir comment on le gèrerait. Pour nos informaticien et nos opérateurs, c'est simple parce qu'ils peuvent travailler de chez eux, donc finalement le site secondaire n'est pas si important. C'est ce qu'on ferait avec un travail à distance et c'est ce qui s'est déjà passé avec un problème de DSL pendant deux jours on a pas pu travailler et les collaborateurs sont restés chez eux pendant deux jours pour travailler à distance…

Est-ce que c'est une durée acceptable pour vous ?

Non lorsqu'il y a un événement critique tel une coupure électrique une coupure réseau qui n'est pas de notre responsabilité on peut le faire entendre aux clients en leur disant ça ne va pas revenir l'année prochaine. En revanche si ça arrive plusieurs fois on pourrait nous reprocher de ne pas savoir gérer ces risques ; par exemple, si tous les 3 ans on a un incendie les clients nous diraient qu'on sait pas gérer ce risque il y a sans doute un problème, etc etc… Je sais qu'on a quand même ce truc ou on se sert un peu d'Orange où le délai de rétablissement c'est 4 heures on fait la même chose pour nos clients. En 15 ans on a eu deux incidents de cette nature…

Si on prolonge cette réflexion pourquoi raisonner autour d'une indisponibilité du site alors que vous avez des solutions pour travailler à distance ?

Parce que la société se développe et évolue vers sa maturité et donc au fur et à mesure on intègre de plus en plus des risques et on a les capacités aussi humaines, économiques de pouvoir en prendre d'autres et puis comme j'ai dit, dans les autres locaux, nous on aurait quelque chose de grave localement, notre solution c'est de renvoyer les gens chez eux pour des questions aussi climatiques. Donc c'était géré mais pas géré comme nos clients le souhaiteraient on pourrait donc avoir ce deuxième site parce que même dans la sécurité il y a des choses qui font partie de l'image, du discours, du marketing et le fait d'avoir un deuxième site permettrait d'alimenter cette image notamment c'est ce qu'on a fait quand on a communiqué le fonctionnement sur multi Data Center et multi opérateur c'est vraiment ça le point sur lequel on a avancé et sur lesquels nos concurrents ne sont pas forcément très engagés… parce que quand vous n'avez qu'un opérateur, ou un data center ce n'est pas suffisant pour présenter le dysfonctionnement au client. Par exemple nos concurrents qui ne sont pas multi site et multi data center, lorsqu'ils ont besoin de basculer, rencontrent souvent des dysfonctionnements : nous on le voit parce que quand les opérateurs coupent les liaisons nos bascules se font automatiquement. Par exemple chez OVH ils ont des problèmes environ tous les 18 mois, un incident majeur, tous les 18 mois c'est beaucoup alors que pour nos clients c'est transparent donc il faut avoir cette capacité dire on bascule dans un data center mais hors de leur périmètre d'influence…

En synthèse toutes c'est mesures que vous avez mise en place visent à couvrir quel risque ?

Nous c'est de pas pouvoir rendre le service attendu par nos clients en premier. Le deuxième c'est ne pas garantir les données de nos clients donc l'accès et aussi la sécurité des données ça c'est la deuxième chose . En plus aujourd'hui on a nos clients mais le système d'information est aussi ouvert sur les clients de nos clients voir quelques fois encore au-delà… donc si il y a un incident important la chaine est assez importante et plus c'est important plus quand ça tape, ça tape de plus en plus fort sur le retour sur incident et quand on a des incidents, on a eu effectivement des

remontées de centre d'appels des clients où il fallait presque gérer leur crise de larmes « je vais les perdre », c'était dramatique. Donc c'est d'ailleurs un peu pour ça aussi que non seulement on met en place un système de secours on va passer de l'opérateur à l'autre mais nos clients sont aussi répartis sur le data center et qu'un incident puisse ne toucher qu'une partie de l'activité c'est surtout pour des questions de gestion de l'incident lui-même parce qu'il y a une vraie partie de la relation client à avoir dans ces cas-là, donc là on divise les risques entre guillemets… Donc quand on a un incident il est gérable en termes de taille même s'il est plus rare mais le jour où on va dire on était tous sur le même opérateur le jour où il y a un incident là il peut y avoir un vrai problème parce qu'on pourrait se retrouver dans l'incapacité de gérer l'incident…

En synthèse aujourd'hui si vous vous posez la question de la sécurité ce serait pourquoi faire ?

Aujourd'hui la sécurité est un mot qui est très utilisé mais on l'a mise dès le départ dans ce qu'on a fait pour le nouveau service c'est la sécurité « by design » tel qu' avec les données exactement

Pour moi sécurité « by design » signifie que ça commence par cet engagement client cet engagement de disponibilité elle commence par là et au fur à mesure de cet engagement de disponibilité on a l'engagement sur la confidentialité et la sureté des données, on décline et on va sur la sécurité suite à des attaques externes, on continu et on prend aussi les attaques internes et on continue et après on est plu sur des attaque on est sur le risque climatique, électrique etc… et on poursuit. Et aujourd'hui on va même au-delà on va prendre en compte aujourd'hui le risque de l'accès licite comme les robots où il faut pouvoir assurer la protection de la donnée parce qu'autant avant la RGPD c'était pas le cas, et maintenant je pense quand même qu'il y a une responsabilité sur les données piratées par ce biais là. Et je sais même pas, je présuppose que si je le détectais je serais normalement obligé de le déclarer… Avec l'essor des technologies on a des risques qu'on couvre aujourd'hui et qui sont bien couverts et au fur et à mesure on essaye d'aller de plus en plus dans les détails…

On a une façon de diffuser le service qui repose sur la sécurité par des systèmes qui ne sont plus dans nos locaux on a des systèmes qui sont retombées la disponibilité de

par l'architecture, disponibilité au sens large est vraiment la plus importante et couvre beaucoup plus de points que juste l'accès lui-même

Par rapport aux décisions que vous prenez pour la sécurité est- ce que dans ces phases de reconnaissance des produits vous observer des éléments qui vous éclaire sur les risques potentiels ?

C'est juste une solution qui s'inscrit par rapport à des besoins identifiés. C'est pas la recherche entre guillemets sur la sécurité qui m'amène à me dire qu'il faut que je fasse ça c'est plutôt je constate cela ou je présent cette difficulté et je veux y répondre et qu'est-ce que je vais proposer comme solution pour y répondre..

Je vous remercie beaucoup pour ces échanges. Est-ce que vous souhaitez apporter un complément d'information sur les sujets que nous avons abordés ou des sujets connexes à la sécurité des SI ?

…. j'ai fait Saint-Cyr et je pense qu'il ressort quelque chose… Après, il y a une chose de très intéressant sur la partie sécurité. Quand j'ai monté l'entreprise, même si je savais quoi faire au niveau architecture, je suis rentré dans un centre de formation pour la création d'entreprise, et là-dedans ils ont fait intervenir un consultant de la DST qui nous a parlé de la sécurité justement dans les grandes lignes. Son grand jeu était de prendre le TGV et quand quelqu'un partait s'acheter une bricole , à boire autre chose, soit il allait piqué son PC soit il allait y faire quelque chose dessus pour montrer son accessibilité… et surtout quand il se rendait compte que c'était de grandes entreprises regardait comment il se comportait et allait leur en parlait pour les sensibiliser… et c'est vrai que ce discours de dire que la sécurité et notamment dans les TPE/PME, n'est vraiment pas pris en compte parce que ça peut être chiant et contraignant et cher dans un deuxième temps… et même par rapport à mes collaborateurs plus d'une fois il faut former, changer les équipements et les logiciels, c'est un petit peu pénible et même pour nous par exemple quand il faut accéder à un site qui n'est pas dans la base du FW il faut demander l'ouverture de l'accès avec des petites contraintes qui permettent de donner l'information au FW mais il n'empêche qu'il y a quelques fois des petits couacs et c'est vrai que du coup ça peut motiver l'informaticien à prendre un petit VPN pour contourner ces mesures de protection

Donc que j'ai été sensibilisé un petit peu par ce discours et ça c'était vachement bien je ne sais pas si les autres ont été aussi sensibilisés que moi mais en tous les cas moi je l'ai reconnu…

Et franchement, après, la grosse difficulté c'est de le faire passer auprès des collaborateurs.. ça c'est un combat de tous les jours encore plus avec les jeunes avec leur téléphone portable. Nous ici tout monde le sait, personne ne doit utiliser de clé USB et si je le vois ils savent que ça va très très mal se passer avec quelques bonnes colères sur le sujet le message est vraiment passé.

Et même un moment on a eu, bon c'était une bonne intention, une opératrice qui a eu une panne Internet et elle a dit elle a utilisé son téléphone pour se connecter et continuer de travailler donc ça c'est des erreurs qui arrivent fréquemment régulièrement et ça les collaborateurs, même informaticiens ont du mal à comprendre les risques liés à mettre un périphérique, clé USB. C'est loin d'être simple…

Merci pour cet échange et votre disponibilité