Université de Montréal

La gestion des risques informationnels dans l'entreprise privée : perspective des gestionnaires de la sécurité.

Par
Chantal Desroches

École de criminologie
Faculté des arts et sciences

Mémoire présenté à la Faculté des études supérieures
Pour l'obtention du grade
M. Sc. en criminologie

Octobre 2013

Université de Montréal

Ce mémoire intitulé :
La gestion des risques informationnels dans l'entreprise privée :
perspective des gestionnaires de la sécurité.

Par
Chantal Desroches

A été évalué par un jury composé des personnes suivantes :

Massimiliano Mulone

Benoit Dupont

Karine Côté-Boucher

Résumé

Ce mémoire de maîtrise porte sur la gestion des risques informationnels dans l'entreprise privée. Plus précisément, nous avons cherché à comprendre, à partir de l'expérience et du point de vue des gestionnaires de la sécurité, comment s'élaborait une prise de décisions relativement à la protection des actifs informationnels d'une entreprise, de l'identification des risques à la mise en place de mesures visant à les réduire. Pour ce faire, nous devions dégager les éléments du contexte organisationnel qui contribuent à façonner les décisions du gestionnaire de la sécurité en cette matière en considérant deux principales dimensions : la dynamique relationnelle à l'œuvre de même que les enjeux, les contraintes et les opportunités susceptibles d'influence la prise de décisions. Nous voulions également connaitre le rôle et les responsabilités du gestionnaire de la sécurité au sein de ce processus décisionnel et préciser, le cas échéant, sa participation au modèle de gouvernance de gestion des risques. Pour rendre compte de la complexité de ce processus, il semblait approprié de concevoir un cadre théorique combinant deux approches: l'approche multidimensionnelle du risque et l'approche de la transaction sociale. Si la première considère que la définition du risque doit être contextualiser, l'autre admet que la dynamique relationnelle n'est pas le simple fait de jeux entres acteurs stratégiques. L'analyse en fonction de ses deux approches a révélé que la gestion des risques informationnels dans une entreprise est largement tributaire des caractéristiques personnelles du gestionnaire de la sécurité. Certes, le contexte organisationnel et la multiplication des enjeux sécuritaires exercent une influence considérable sur le processus décisionnel mais l'expérience, les connaissances et les capacités communicationnelles du gestionnaire contribuent directement à la réussite de chaque phase du processus de gestion des risques informationnels.

Mots clés : sécurité, gestion, risques informationnels, entreprise, protection des actifs, approche multidimensionnelle du risque, approche de la transaction sociale.

Abstract

This master is about the informational risk mitigation within the private sector. More precisely, we have tried to understand, from the experience and the point of view of the security managers, how was the decision making process elaborated with regards to the protection of the informational assets. In order to achieve this, we had to take the elements, which are influencing the decisions taken by the security managers with regards to this subject matter, out of its organizational context and consider two main dimensions: the relational dynamics at play and the issues, constraints, and opportunities likely to influence the decision making.

We wanted to know as well, what were the roles and responsibilities of the security managers with in the decision making process and determine their participation in the security governance model. To expose the level of complexity of this process, we thought it would be appropriate to create a theoretical frame work combining two different approaches: the multidimensional approach and the social transaction approach. If the first one considers that the risk definition needs to be put in a context, the second one admits that the relationship dynamics are not just a simple power game between strategic actors. The analysis of the two approaches has revealed that the informational risk mitigation in the private sector is largely tributary to the personal characteristics of the security managers. More so, the organisational context and the rising numbers of security treats are considerably influencing the decision process, but the experience, the knowledge and the communication skills of the security managers are directly contributing to the success of each phase in the informational risk mitigation process.

Key words : security, risk management, organisation, asset protection, information risk, multidimensional risk approach, social transaction perspective.

TABLE DES MATIÈRES

RÉSUMÉ ..... **i**

ABSTRACT ..... **ii**

LISTE DES TABLEAUX, FIGURES ET ABRÉVIATIONS ..... **v**

REMERCIEMENTS ..... **vi**

1. INTRODUCTION **1**

2. RECENSION DES ÉCRITS **5**

2.1 LE RISQUE : PRINCIPES D'APPLICATION **7**

2.2 LA GESTION DU RISQUE DANS L'ENTREPRISE **10**

2.3 LA GESTION DU RISQUE INFORMATIONNEL **12**

2.3.1 LE PATRIMOINE MATÉRIEL ET IMMATÉRIEL **12**

2.3.2 LE RISQUE INFORMATIONNEL ET LA SÉCURITÉ DE L'INFORMATION **14**

2.3.3 LES RISQUES ASSOCIÉS AUX NOUVELLES TECHNOLOGIES **16**

2.3.4 LA PROTECTION DU PATRIMOINE INFORMATIONNEL DANS L'ENTREPRISE **18**

2.4 LE GESTIONNAIRE DE LA SÉCURITÉ DANS L'ENTREPRISE **20**

2.4.1 RÔLES ET RESPONSABILITÉS DES GESTIONNAIRES DE LA SÉCURITÉ EN MATIÈRE DE GESTION DES RISQUES INFORMATIONNELS **20**

2.4.2 CARACTÉRISTIQUES PERSONNELLES DU GESTIONNAIRE **25**

2.4.3 LA PLURALITÉ DES ACTEURS : RÉSEAUX **26**

2.4.4 COLLABORATION, NÉGOCIATION ET SYNERGIE **28**

2.5 CADRE THÉORIQUE **30**

2.5.1 PROBLÉMATIQUE ET OBJECTIFS DE LA RECHERCHE **34**

3. MÉTHODOLOGIE **37**

3.1 LA MÉTHODE QUALITATIVE **38**

3.1.1 ENTRETIENS SEMI-DIRECTIFS **39**

3.1.2 ENTRETIENS EXPLORATOIRES **40**

3.2 ÉCHANTILLONNAGE **41**

3.2.1 CARACTÉRISTIQUES DE L'ÉCHANTILLON **44**

3.2.2 PROFILS DES RÉPONDANTS **45**

3.3 CUEILLETTE DE DONNÉES **46**

3.3.1 CONDITION DE RÉALISATION DES ENTRETIENS **46**

3.3.2 CADRE CONTRACTUEL DE L'ENTRETIEN **48**

3.4 STRATÉGIE ANALYTIQUE **49**
3.5 LIMITES **50**

4. ANALYSE **52**
4.1 L'ASPECT CONTEXTUEL **54**
4.1.1 DE QUEL TYPE D'ENJEUX EST-IL QUESTION? **54**
4.1.2 CONTRAINTES ET OPPORTUNITÉS **60**
4.1.3 TOLÉRANCE AU RISQUE **63**
4.2 L'ASPECT RELATIONNEL **64**
4.2.1 AU SEIN DE L'ENTREPRISE **64**
4.2.2 À L'EXTERNE : UNE QUESTION DE NÉCESSITÉ **70**
4.2.3 RÉSEAUX **74**
4.3 PROFIL DU GESTIONNAIRE **78**
4.3.1 RÔLE ET RESPONSABILITÉS **78**
4.3.2 CHEMINEMENT DE CARRIÈRE **81**
4.3.3 DE QUELS OUTILS DISPOSENT-ILS? **85**
4.4 IDENTIFICATION ET HIÉRARCHISATION DES RISQUES **90**
4.5 PROFITABILITÉ DE L'ENTREPRISE ET SÉCURITÉ: OBJECTIFS INCONCILIABLES? **93**

5. LA GESTION DES RISQUES INFORMATIONNELS À TRAVERS DEUX APPROCHES: LA TRANSACTION SOCIALE ET L'APPROCHE MULTIDIMENTIONNELLE DU RISQUE **96**
5.1 DE LA NÉGOCIATION À LA TRANSACTION SOCIALE **101**
5.2 L'APPROCHE MULTIDIMENSIONNELLE DU RISQUE **104**

6. CONLUSION **108**

ANNEXES

ANNEXE A. CARACTÉRISTIQUES DE L'ÉCHANTILLON
ANNEXE B. SCOLARITÉ ET APPARTENANCE À UN RÉSEAU PROFESSIONNEL
ANNEXE C. THÈMES ET CATÉGORIES

LISTE DES TABLEAUX

TABLEAU 1. LE PATRIMOINE INFORMATIONNEL D'UNE ENTREPRISE 13

TABLEAU 2. ENTREPRISES BRITANNIQUES AYANT SUBI UNE BRÈCHE DE SÉCURITÉ EN 2013 15

TABLEAU 3. DOMAINES D'ACTION DES PROFESSIONNELS DE LA SÉCURITÉ DE L'INFORMATION 21

LISTE DES FIGURES

FIGURE 1. HIÉRARCHIE COGNITIVE 9

FIGURE 2. GESTION DES RISQUES INFORMATIONNELS 106

LISTE DES ABRÉVIATIONS

ABCP	Associate Business Continuity Professional
AQIS	Association Québécoise de l'Industrie de la Sécurité
ASIQ	Association de la Sécurité de l'Information du Québec
ASIS	American Society for Industrial Security
BYOD	Bring Your Own Device
CISSP	Certified Information Systems Security Professional
CQCD	Conseil Québécois du Commerce de Détail
DRI	Disaster Recovery Institute
FIPS	Federal Information Processing Standard
PCI DSS	Payment Card Industry Data Security Standards
PME	Petites et moyennes entreprises
TI	Technologie de l'information

Remerciements

Bien que je souhaiterais énumérer tous ceux et celles qui ont contribué à la réalisation de ce mémoire, je serai brève et je dois d'abord et avant tout remercier ma famille. À mes enfants, qui ont perdu momentanément leur maman et à mon conjoint qui m'a toujours soutenue et poussée de l'avant dans l'accomplissement de cette quête que j'ai cru par moment interminable. Votre amour m'a aidé à persévérer et à atteindre mon objectif. Je vous en serai toujours reconnaissante. Je remercie également chaque membre de ma famille qui a su m'offrir aide et support quand j'en avais le plus besoin. Vous vous reconnaitrez!

Je remercie également ceux qui ont bien voulu croire à ce projet et qui ont accepté, bien généreusement, de me rencontrer et de répondre à mes questions. Sans vous, ce projet n'aurait jamais vu le jour. Je suis aussi reconnaissante pour la patience dont a fait preuve mon directeur de recherche : merci de ne pas m'avoir abandonné…

Finalement, un merci tout particulier à mon patron, mes collègues et mon «partner» qui ont supporté mes crises existentielles, ma mauvaise humeur passagère et mes étourderies...

La route fut longue mais j'y suis arrivée!

CHAPITRE 1. INTRODUCTION

1. Introduction

Pour la plupart d'entres nous, la communication de l'information par voie électronique relève d'une activité banale, presque machinale. Les risques qui découlent de la communication de cette information font toutefois rarement l'objet d'une attention particulière de la part de ceux qui se prêtent à cette activité, même lorsque cette activité a lieu dans un cadre professionnel. D'un point de vue organisationnel, l'avènement des applications en nuage, l'utilisation massive de dispositifs de communication intelligents et la popularité sans cesse croissante des médias sociaux font en sorte que les risques informationnels se multiplient et s'étendent à toutes les activités de l'organisation.

De nombreux articles ont fait état d'une situation qui laissait présager, jusqu'à tout récemment, que la protection de l'information au sein des organisations souffrait de lacunes importantes (Samli & Jacob 2003, Willison 2006, Foryst 2010). Toutefois, depuis les trois dernières années, les entreprises tendent à reconnaitre la nécessité de se prémunir d'outils efficaces pour parer aux risques et malgré les compressions budgétaires liées à une situation économique encore précaire, on remarque une augmentation des budgets consacrés à la protection de l'information (Deloitte; Ernst & Young; PricewaterhouseCoopers)[1]. Les gestionnaires semblent davantage conscientisés quant à la nature et à l'ampleur des menaces auxquelles leurs entreprises sont exposées mais nous en savons encore très peu sur les mécanismes sous-jacents qui permettent d'expliquer ce changement, cette évolution des mentalités.

Et bien que le risque soit l'objet d'une réflexion ayant produit de nombreux écrits à travers différentes disciplines, l'intégration de sa spécificité au sein d'un processus élargi de gestion du risque n'en est qu'à ses balbutiements. Plus spécifiquement, nos connaissances relatives à la gestion des risques informationnels sont encore insuffisantes, notamment en ce qui concerne les PME. En effet, nous faisons face à de multiples

[1] Ces firmes réalisent des enquêtes sur une base annuelle auprès de leurs clients. Dans le cadre de cette recherche, nous avons consulté les rapports de 2009 de la firme Deloitte, les rapports de 2011 à 2013 pour PWC et 2012 pour Ernst & Young.

barrières. D'abord, les données portant spécifiquement sur la gestion des risques informationnels sont difficilement accessibles. Les exigences de confidentialité sont particulièrement élevées et les entreprises n'ont aucun intérêt à dévoiler leurs faiblesses ou encore leurs méthodes de protection. Ensuite, faut-il le souligner, les études de grandes envergures sont dirigées principalement vers les grandes entreprises par l'entremise de questionnaires, nous confrontant ainsi à une perspective qualitative relativement limitée. Il nous est donc difficile, actuellement, de donner un sens à la situation qui prédomine au sein des entreprises privées en matière de gestion des risques informationnels car s'il est possible de dresser un portrait statistique des risques auxquels les entreprises font face, nous en savons encore très peu sur le processus décisionnel qui permet d'identifier et de hiérarchiser ces mêmes risques.

Qui plus est, le rôle du gestionnaire de la sécurité en cette matière nous est pratiquement inconnu. Sachant que la protection des actifs corporatifs constitue la principale préoccupation du gestionnaire de la sécurité, nous ne savons guère où il se situe par rapport à la gestion des risques informationnels. L'information étant en soi un actif corporatif, qui en assure la protection? Confronté à l'émergence de nouveaux risques, la conjoncture technologique a-t-elle, en quelque sorte, transformée la fonction sécurité au sein de l'entreprise, forçant ainsi les gestionnaires à s'adapter ou à se délester de certaines responsabilités? Leur rôle a certes évolué et la vision traditionnelle que nous en avons mérite d'être redéfinie et située à travers une perspective contemporaine (O'Reilly & Ellison, 2006). C'est dans cette optique de recherche que nous nous sommes engagés.

En fait, ce mémoire présente un double objectif : comprendre comment s'effectue la gestion des risques informationnels dans l'entreprise privée et revisiter la fonction «sécurité» en tenant compte de la multiplication des risques qui menacent le patrimoine informationnel des organisations. Pour réaliser ces objectifs, un certain nombre de questions devront se poser. D'abord, existent-ils des processus permettant d'identifier et de hiérarchiser les risques informationnels et si oui, quels sont-ils? Quel est le rôle du gestionnaire de la sécurité en cette matière? S'agit-il d'un rôle passif ou stratégique? En matière de protection de l'information, favorise-t-on encore l'approche compartimentée

ou en silo ou bien, les organisations privilégient davantage les approches intégrées favorisant la coopération et la cohérence des actions entre les intervenants et le gestionnaire de la sécurité?

C'est à partir d'entretiens effectués auprès de gestionnaires de la sécurité et/ou sécurité de l'information que ce travail a été réalisé. Ce travail comporte trois principales sections; le premier chapitre fera état de la littérature qui traite de la gestion du risque en entreprise et de la sécurité des actifs informationnels. Le second chapitre sera consacré à la méthodologie employée pour recueillir et analyser les données. Et finalement, le troisième chapitre présentera une analyse en deux temps; nous débuterons par une analyse tridimensionnelle des données qui tiendra compte de l'aspect contextuel, de l'aspect relationnel et du profil du gestionnaire. Nous procèderons ensuite à une analyse de la dynamique organisationnelle de la gestion du risque à partir d'un cadre théorique conçu spécifiquement à cet effet et qui réuni deux approches : l'approche multidimensionnelle du risque (Kermisch 2012) et l'approche de la transaction sociale Rémy 2005; Eraly 2008; Maroy 2009; Fusulier & Marquis 2009; Bourque & Thuderoz 2011). Cette union s'est d'ailleurs avérée fructueuse puisqu'elle nous a permis d'approfondir l'aspect relationnel sans toutefois négliger l'aspect contextuel du processus de gestion des risques informationnels où conflits, négociations et compromis sont omniprésents dans ce qui constitue le quotidien du gestionnaire de la sécurité.

Ainsi, la pertinence de cette recherche ne réside pas uniquement dans cette nécessité de définir de façon réaliste le rôle du gestionnaire de la sécurité en matière de gestion des risques informationnels. Elle nous permet d'analyser la dynamique relationnelle entre les acteurs et l'influence de ces interactions sur le processus de gestion des risques informationnels. Finalement, à la fin de cette recherche, nous serons en mesure de dégager ce qui représente, selon le point de vue des gestionnaires de la sécurité, une approche organisationnelle efficace et efficiente en matière de gestion des risques informationnels et de protection de l'information.

CHAPITRE 2. RECENSION DE LA LITTÉRATURE

2. Recension de la littérature

La gestion du risque informationnel en entreprise relève d'une discipline relativement récente qui s'est, en quelque sorte, imposée d'elle-même compte tenu de l'évolution des moyens technologiques mis à notre disposition pour traiter et communiquer l'information. Et bien que la gestion des risques, en tant qu'activité managériale, ait fait son apparition vers la fin des années 50, les entreprises souhaitant une alternative à des coûts assuranciels toujours plus élevés (Hassid 2008; Dionne 2013), ce n'est qu'au début des années 80 que la recherche s'éveille aux risques relatifs au développement des sciences et de la technologie (Beck 2001). Les travaux fondateurs de Lagadec (1981) et Douglas & Wildavsky (1982) ont pour ainsi dire, jeté les bases d'une réflexion qu'Ulrich Beck allait poursuivre pour développer ce qu'il nomma la Société du risque (Beck 1986). Issue d'une modernité réflexive, la société industrielle telle que nous la connaissons fait progressivement place à une société productrice de risques qu'elle tente en vain de contrôler (Beck 1986).

Par ailleurs, la nature particulièrement diffuse du concept de risque se voit complexifié par certaines dimensions d'ordre culturel, sociétal, politico-économique et individuel. Par exemple, ce qui représente un risque acceptable pour certains, devient peut-être un risque intolérable pour d'autres. Le concept de risque se transforme aussi dans le temps et l'espace; les risques d'aujourd'hui sont différents des risques d'hier et de demain. Ainsi, si les innovations technologiques ont contribué à réduire considérablement certains risques, notamment dans le domaine de la santé, elles ont aussi conduit à produire de nouveaux risques comme les risques biologiques ou nucléaires; conséquences mitigées qui sont constatées à travers diverses sphères de la société. Et même si le concept de risque peut endosser une connotation positive du fait que le résultat d'un choix (le choix de prendre un risque), pourrait être générateur de réussite ou de succès et non d'échec ou de danger, le risque comporte indubitablement une connotation négative qui nous renvoie soit à une menace potentielle, soit à un danger imminent ou encore à une conséquence malheureuse (Slovic 2002; Kermisch 2012).

Cette perspective contraint les individus et les organisations à réduire leur exposition aux risques ou à tout le moins, à tenter de contrôler ces risques (March & Shapira 1987; Klinke & Renn 2002). La première section de ce chapitre sera d'ailleurs consacrée à la compréhension du risque dans un contexte organisationnel. Comme le mentionne l'intitulé de ce mémoire, il sera plus particulièrement question, dans les sections ultérieures de ce même chapitre, de la gestion des risques informationnels et de la sécurité de l'information. Finalement, notre attention se portera vers le gestionnaire de la sécurité, son rôle, ses responsabilités et ses interactions avec les différents acteurs qui interviennent dans le processus de gestion des risques informationnels.

2. 1 Le risque : principes d'application

Revenons d'abord sur cette nécessité de contrôler ou de réduire un risque. Cette opération implique nécessairement de déterminer ou d'évaluer la probabilité d'occurrence dudit risque. Pour ce faire, le calcul du risque s'effectuera à partir de deux éléments : la probabilité qu'un évènement se produise et l'ampleur des conséquences (sévérité du risque) liées à cet évènement (Kaplan et Garrick, 1981). Si les conséquences peuvent être objectivables (mathématiquement quantifiables), les probabilités, quant à elles, ne peuvent être qu'estimées (Beck 2001; Slovic 2002; Kwak & Laplace 2005; Kermish 2012). Qui plus est, le concept de risque de par sa subjectivité est difficile à circonscrire puisque «d'un point de vue ontologique…le risque n'existe pas» (Kermisch 2012, p.1). «It does not exist "out there," independent of our minds and cultures, waiting to be measured. Instead, risk is seen as a concept that human beings have invented to help them understand and cope with the dangers and uncertainties of life» (Slovic 2002, p.4). Il est d'autant plus difficile d'identifier un risque et d'en estimer l'impact si l'objet du calcul n'existe que virtuellement.

C'est pourquoi deux approches se confrontent lorsqu'il est question aborder le risque et d'en argumenter les principes : l'approche constructiviste et l'approche réaliste. La

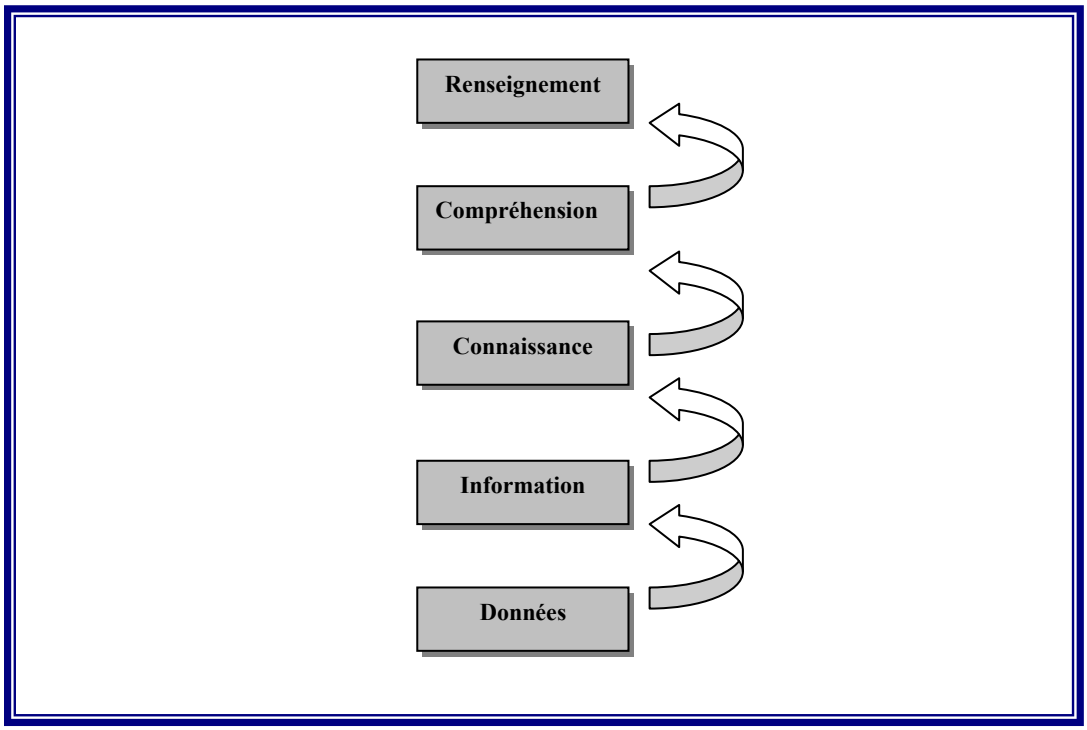
première conçoit le risque comme une construction mentale «that can be check at best against standards of consistency, cohesion and internal conventions of logical deduction» (Klinke & Renn 2002, p.1073). La seconde approche prétend que les calculs mathématiques ou économétriques constituent des méthodes suffisamment objectives pour estimer le risque et pour projeter une image réaliste de sa matérialisation potentielle (Klinke & Renn 2002; Kermish 2012). Dans une étude réalisée auprès de gestionnaires du risque au sujet de la façon de quantifier le risque, March et Shapira (1987) rapportent que 42% d'entre eux sont convaincus que «…there was no way to translate a multidimensional phenomenon into one number» (p.1408). Bien que cette étude ait été effectuée en 1986, le débat est loin d'être clos et les deux approches demeurent fortement critiquées (Kermish 2012), puisque si l'une ignore la dimension subjective liée à la représentation ou à la perception du risque, l'autre néglige l'apport des méthodes quantitatives pour calculer et prévenir ces mêmes risques.

Dans une perspective de gestion des risques, l'objectif demeure cependant le même : réduire le risque à la source ou en contrôler les effets indésirables. Klinke et Renn (2002) ajoutent que indépendamment de l'approche utilisée, trois obstacles se rencontrent lorsqu'il est question d'identifier des risques, de les hiérarchiser et de tenter de les maîtriser : «la complexité, l'ambigüité et l'incertitude» (Klinke & Renn 2002, p.1085). La complexité réfère à la difficulté de saisir les liens causals et les interactions entre une multitude de variables répondant à des logiques distinctes. L'ambigüité est liée aux différentes interprétations dont peut être sujet un même fait ou une même information. Tandis que l'incertitude fait référence aux variations statistiques, aux erreurs d'évaluation ou encore à l'ignorance (variables encore inconnues). Selon Klinke et Renn (2002), plus les niveaux d'incertitude et de complexité sont élevés, plus l'identification d'un risque et l'interprétation de ses effets deviennent ambiguës.

C'est la raison pour laquelle les notions de connaissance et d'information doivent être considérées lorsqu'il est question de gestion des risques (Alexandre-Leclair 2001; Harbulot & Moinet 2002; Bulinge 2002; Danielson 2009; Klinke & Renn 2002). Il n'est toutefois pas aisé de distinguer l'information du renseignement et encore moins de

déterminer ce qui constitue une connaissance ou un savoir. Ce que D.W. Knight (2004) appelle la «hiérarchie cognitive» illustre de façon succincte le processus par lequel l'information est transformée pour potentiellement, devenir du renseignement[2].

Figure 1. Hiérarchie cognitive



Les concepts de donnée, d'information, de connaissance et de savoir abordés par Brodeur dans un chapitre traitant du renseignement (2007) s'intègrent de façon naturelle dans ce processus. Brodeur insiste par ailleurs sur l'hypothèse que «le renseignement n'est pas un objet qui tient sa spécificité de ses caractères intrinsèques mais plutôt de ses propriétés relationnelles» (Brodeur 2007, p. 264). C'est-à-dire que la masse d'informations triée et structurée en renseignement se réalisera «au sein d'un processus dynamique d'échange» (Brodeur 2007, p. 269). D'un point de vue organisationnel, c'est à travers ce processus que s'opère l'appréciation subjective des risques informationnels,

[2] Tiré de Cox, Jim (2009). Le renseignement : définitions, notions et gouvernance. *Service d'information et de recherche parlementaires, division des affaires sociales*.

aussi nécessaire qu'une quantification objective peut l'être dans une gestion des risques qui se veut optimale (Léger 2008).

2.2 La gestion du risque dans l'entreprise

La gestion du risque en tant que concept mais aussi en tant qu'activité managériale, a été au centre de nombreuses recherches et a fait l'objet d'une multitude de définitions (March & Shapira 1987; Léger 2004)[3]. Le caractère spécifique de cette fonction combiné à la diversité des risques auxquels l'entreprise peut faire face en complique la tâche. «Complexe et multidimensionnel, le concept de risque occupe dorénavant une place centrale dans toute organisation» (CIRANO 2005, p.1)[4] et parce que chaque entreprise évolue au sein d'un environnement qui comporte un certain nombre de contraintes qui lui sont propres, elle fait face à l'obligation de poser un double diagnostic, celui de son environnement externe et celui de son environnement interne.

L'environnement externe d'une entreprise est constitué du contexte règlementaire (normes, standards, lois, règlements), du contexte technologique et sociopolitique, de ses clients, de ses fournisseurs, de ses partenaires (banques, firmes-conseils, associations, comités, ordre professionnel), de ses compétiteurs, des médias et des groupes de pression pour ne nommer que ceux-là. Au sein même de l'entreprise, nous retrouvons, entre autres, la direction et le conseil d'administration, les ressources humaines, financières, opérationnelles et légales ainsi que les syndicats. La nature des activités de l'entreprise, sa culture organisationnelle et son mode de gouvernance s'avèrent aussi essentiels lorsqu'il est question de faire l'analyse de l'environnement d'une entreprise. Cette analyse débute cependant par une prise de conscience des enjeux, qu'ils soient technologiques, humains ou sécuritaires et par la mise en œuvre d'un

[3] Ces auteurs ont compilé une série d'approches théoriques et méthodologiques au sujet de la gestion du risque.
[4] CIRANO : Centre interuniversitaire de recherche en analyse des organisations.

processus qui intègre tous les niveaux de l'organisation (COSO 2005; Ebondo Wa Mandzila & Zéghal 2009). De la gestion du risque, nous pouvons retenir deux définitions: «Risk management is a process, a theory, a procedure, or a methodology for determining your assets, vulnerabilities, and threats and then, protecting them» (Roper 1999, p.304). La définition qui nous semble la plus complète et qui semble refléter davantage la réalité organisationnelle des entreprises d'aujourd'hui est sans doute celle élaborée par COSO *(*Committee of Sponsoring Organizations of the Treadway Commission) :

> «Le management des risques est un processus mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation» (COSO 2005, p.3).

Ce processus se divise généralement en trois étapes. La première étape vise à définir le contexte organisationnel : les objectifs de l'entreprise, ses stratégies, sa structure et sa tolérance au risque (Shedden & al. 2011). La tolérance au risque ou l'appétence pour le risque «fait référence au degré de risque qu'une organisation est capable d'accepter» (Ebondo Wa Mandzila & Zéghal 2009, p. 19). Puisque tous les risques ne peuvent être éliminés, les gestionnaires seront forcés de faire des choix et ces choix seront déterminés en partie par l'appétence pour le risque des dirigeants, variable indissociable des autres éléments du contexte organisationnel.

La deuxième étape de la gestion des risques consiste à identifier lesdits risques. Lajili et Zéghal, en 2005, distinguaient quinze catégories de risques. En 2009, Zéghal reprend cette catégorisation pour maintenant parler de quatre grands risques : les risques

stratégiques, opérationnels, règlementaires et informationnels (Ebondo Wa Mandzila & Zéghal 2009, p.19). Dans cette recherche, nous nous intéresserons principalement aux derniers. Quant à la troisième étape du processus de gestion des risques, il s'agit de procéder à une analyse de risque à l'aide de différents outils méthodologiques auxquels nous ne nous attarderons pas dans ce travail. Cette analyse de risques consiste à déterminer la probabilité qu'un évènement se produise par rapport à l'impact que ce même évènement pourrait avoir sur les activités de l'entreprise et par conséquent, de quelle façon il affecterait l'intégrité des actifs de cette dernière. Ces trois étapes amène le gestionnaire à hiérarchiser les risques et à déterminer quelles actions doivent être privilégiées : l'évitement, la réduction, le transfert ou l'acceptation (Whitman & Mattord 2005; Ebondo Wa Mandzila & Zéghal 2009; Shedden & al. 2011).

De fait, il n'existe point de modèle prédéterminé ni de guide du parfait gestionnaire (Klinke & Renn 2002). Si la gestion du risque suppose l'élaboration d'une stratégie adaptable et intégrée, elle suppose aussi une connaissance approfondie de l'environnement concurrentielle et une maîtrise optimale de l'information stratégique (Pépin, 2007). Pour Ebondo Wa Mandzila et Zéghal (2009), «il s'agit d'une approche rigoureuse de l'évaluation et du repérage de tous les risques menaçant l'atteinte des objectifs stratégiques d'une organisation» (p.18). La gestion des risques en entreprise se voit donc intrinsèquement liée aux objectifs que poursuit l'organisation et doit être pensée en partie, en fonction de ces derniers.

2.3 La gestion du risque informationnel

2.3.1 Le patrimoine matériel et immatériel

Une gestion des risques efficace implique aussi d'identifier ce qui constitue le patrimoine informationnel de l'entreprise. Le patrimoine informationnel peut être défini comme «l'ensemble des données et des connaissances, protégées ou non, valorisables ou

historiques d'une personne physique ou morale» (Livre Blanc CIGREF 2007). Ces données et connaissances sont classées en trois différents types d'information : l'information blanche accessible au grand public par l'entremise de sources ouvertes, généralement non protégée; l'information grise dont l'accès est restreint et protégé; et enfin, l'information noire, secrète dont l'accès est strictement limité à certains individus clés de l'organisation (Bulinge 2002; Morizot 2011). Le patrimoine informationnel regroupe une quantité innombrable d'éléments dont une liste exhaustive ne pourrait être dressée dans le cadre de cette recherche. Toutefois, le tableau proposé par Hervé Morizot (2011) résume de façon concise de quoi peut être constitué le patrimoine informationnel d'une entreprise.

Tableau 1. Le patrimoine informationnel d'une entreprise

• **Le savoir faire de l'entreprise** o Les méthodes de distribution, les brevets, les procédés de fabrication o Les projets stratégiques à venir
• **Les informations commerciales** o La stratégie commerciale o La typologie de mes clients (qui achète quoi, pourquoi, etc.)
• **Les informations sur le personnel de l'entreprise** o Informations RH o L'état de santé des dirigeants o La formation de mon personnel, les personnes clés dans l'entreprise.
• **Les partenaires de l'entreprise** o Les fournisseurs, les sous-traitants, les clients, les consultants…
• **Les informations financières** o Chiffres clés, marge, ventilation du CA par activité, niveau de trésorerie…
• **Les informations juridiques** o Les contentieux en cours o Le positionnement légal de l'entreprise.

Tiré d'Hervé Morizot (2011). L'intelligence des risques

L'information doit aussi être considérée à travers deux types d'actifs : le patrimoine immatériel, constitué principalement de données informatisées et le patrimoine matériel dans lequel nous retrouvons les personnes et les biens (locaux, systèmes d'information, échantillons, maquettes, documents confidentiels, etc.) (CDSE, commission IE 2010).

Larivet (2009) suggère par ailleurs que la protection de l'information se divise généralement en deux catégories : a) les compétences et connaissances détenues par l'entreprise et b) les informations émises par l'entreprise (révélatrices de sa stratégie). La manière de catégoriser le patrimoine informationnel dépend de plusieurs facteurs d'ordre organisationnel mais son objectif demeure le même : connaître ce qui doit être protégé.

Ainsi, l'une des principales difficultés «en matière de gestion des risques et de leur transfert tient dans la qualification des objets informationnels et de l'identification des flux d'échanges entre les différents acteurs» (Santoni 2006 p.1). Selon une étude portant sur la sécurité informatique et la valeur des écrits au travail, les entretiens ont révélés que tant qu'un document n'est pas qualifié de stratégique ou de confidentiel, sa valeur reste floue aux yeux des usagers (Denis 2009). D'une part, les répondants croient que les données brutes sont inutiles et sans valeur pour les concurrents puisqu'elles sont dépouillées de leurs sens (du contexte dans lequel elles ont été produites). D'autre part, on minimise la perte de documents en prétextant leur duplication à travers l'organisation. Nous nous retrouvons donc face à un bien informationnel mal protégé car mal défini et dont la valeur reste inconnue. La gestion des risques informationnels en est d'autant plus ardue. Et bien qu'il existe de nombreuses façons de concevoir la notion de patrimoine informationnel, il importe toujours d'identifier les éléments qui représentent des actifs stratégiques pour l'entreprise pour ainsi déterminer en quoi ceux-ci peuvent contribuer à acquérir un avantage concurrentiel (CIGREF 2007). Dès lors, il est possible d'orienter les activités de sûreté et de sécurité en fonction d'objectifs clairs et réalisables : ce qui d'ailleurs constitue l'un des éléments centraux de cette recherche.

2.3.2 Le risque informationnel et son potentiel de matérialisation

L'information est certes une source d'avantage concurrentiel mais elle demeure très souvent une source de risque : c'est ce que nous appelons le risque informationnel. «La notion de risque informationnel est née avec l'avènement de l'information dont l'exploitation stratégique constitue désormais une réalité et un enjeu pour les

organisations» (Harbulot, Moinet & Lucas 2002, p.9). Les progrès technologiques, notamment au niveau d'Internet, font désormais en sorte que le flux d'information augmente de façon exponentielle, décuplant du même coup les risques qui en découlent. D'autant que le risque informationnel peut provenir de différentes sources, ces sources se situent autant dans l'environnement interne de l'entreprise que dans son environnement externe. À l'interne, les risques sont principalement liés à une communication de l'information non maîtrisée c'est-à-dire qu'il y a peu ou pas de mécanismes de contrôle de l'information, que ces mécanismes sont inefficaces, qu'ils ne sont pas appliqués de façon systématique ou encore, plus simplement, que les employés ne sont pas en mesure de distinguer l'information publique de l'information confidentielle. À l'externe, nous parlons principalement de l'atteinte à l'image ou à la réputation de l'entreprise et de la désinformation. Le risque informationnel peut aussi résulter de la pression exercée par certains groupes (les lobbyistes ou les groupes syndicaux par exemple), de la divulgation volontaire d'informations sensibles, de rumeurs et bien sûr, de la perte ou du vol de biens informationnels physiques ou virtuels (Delbecque, E. 2008; Morizot 2011; Dupont 2010). Le risque informationnel revêt plusieurs formes et sa matérialisation, lourde de conséquences, touche tant les grandes entreprises que les PME. Le tableau suivant, tiré d'une étude menée par PricewaterhouseCoopers nous renseigne sur le pourcentage des entreprises britanniques ayant subi une attaque de leur système informatique en 2013[5].

Tableau 2. Entreprises britanniques ayant subi une brèche de sécurité en 2013

NATURE DE L'ATTAQUE	PME	GRANDES ENTREPRISES
Intrusion informatique	33%	55%
Virus informatique, logiciel malveillant	45%	73%
Déni de service	16%	38%
Tentative de pénétration du système informatique	12%	24%
Vol de propriété intellectuelle	4%	16%

[5] 2014 Information Security Breaches Survey. PWC. Department for Business Innovation and Skills. United kingdom.

Dans cette étude, il est également intéressant de constater qu'une part non négligeable des brèches à la sécurité de l'information est due au comportement des employés. En effet, en 2013, 58% des grandes entreprises britanniques ont vécu les répercussions du comportement malveillant ou négligeant de leurs employés, contre 22% pour les PME. PWC note cependant une baisse significative par rapport à l'année précédente (baisse respective de 25% et 50%) et précise par le fait même qu'une meilleure communication des risques et une sensibilisation accrue auprès des membres de l'exécutif permet d'anticiper une réduction de ce type d'incident dans le futur.

Bien que le comportement des employés soit une source d'inquiétude pour les gestionnaires de la sécurité, les risques d'intrusion et/ou de vol de données provenant d'un utilisateur externe non autorisé sont bien réels. La firme de télécommunication Verizon a d'ailleurs identifié lors d'une enquête pour laquelle ont été mises à contribution les données de 50 organisations réparties à travers le monde, neuf types d'incidents qui correspondent à 94% de tous les incidents répertoriés[6] : outre des erreurs diverses commises par les utilisateurs des systèmes informatiques, la malveillance à l'interne et l'abus de privilèges, l'enquête montre que les risques se sont matérialisés à travers les programmes malveillants, la perte ou le vol de données matérielles, les attaques via les applications web, les attaques par déni de service, le cyber espionnage, les intrusions par les points de vente en magasin et le vol et/ou le clonage de cartes bancaires. Et bien que la proportion des incidents varie d'une industrie à l'autre, le total de ces incidents, qu'ils proviennent de l'interne ou de l'externe ne cessent d'augmenter depuis les trois dernières années.

2.3.3 Les risques associés aux nouvelles technologies

L'utilisation des nouvelles technologies n'est pas étrangère au pourcentage élevé d'incidents répertoriés au sein des entreprises. L'étude réalisée par PWC[7] nous informe

[6] Verizon 2014 Data Breach Investigations Report.
[7] 2014 Information Security Breaches Survey. PWC. Department for Business Innovation and Skills. United kingdom.

que dans 7% des organisations, les brèches à la sécurité de l'information étaient liées aux téléphones intelligents et aux tablettes alors que 5% d'entre elles relevaient d'incidents dus à une gestion inadéquate des applications en nuage. Quant aux médias sociaux, 12% des organisations ont constaté une divulgation non autorisée de renseignements ou des indiscrétions de la part de leurs employés.

Ce qui surprend davantage, c'est qu'au sein de nombreuses entreprises, les politiques de sécurité permettant de contrôler l'utilisation des appareils mobiles, des applications en nuage ou des médias sociaux sont quasi inexistantes. À titre d'exemple, la firme Ernst & Young rapportait que 30% des entreprises sondées utilisaient les applications en nuages en 2010 comparativement à 59% en 2012. De ce nombre, «38 % des répondants ont déclaré que leur entreprise n'avait mis aucun contrôle en œuvre pour limiter les risques liés à l'utilisation du cloud» (Ernst & Young 2012)[8]. Le Rogue IT constitue également un problème puisqu'il est possible d'utiliser les fonctionnalités du «cloud» sans passer par le processus d'approbation IT. On constate une problématique similaire avec les politiques BYOD (Bring your own device). Encore une fois, qu'il s'agisse de tablettes ou de téléphones intelligents, la gestion de ces appareils ou leur niveau de sécurité et d'encryptage sont laissés à la bonne volonté des employés qui les utilisent. Les études de PricewaterhouseCoopers, Deloitte et Ernst & Young indiquent par ailleurs que les risques liés aux réseaux sociaux font davantage l'objet de contrôles et de politiques de sécurité: accès inexistants ou limités, sensibilisation des employés, surveillance des sites et mesures disciplinaires (Ernst & Young 2012).

En résumé, les nouvelles technologies ouvrent bien évidemment les portes à de nombreuses opportunités : augmentation du niveau de productivité, motivation des employés et réduction des dépenses technologiques (Ernst & Young 2012). Cependant les entreprises, témoins de leur incapacité à s'adapter au rythme effréné de l'évolution de ces technologies et du même coup, à contrôler efficacement les risques informationnels n'ont d'autres choix que d'adapter leurs stratégies en optant pour des solutions centrées

[8] Ernst & Young's 2012 Global Information Security Survey.

davantage sur l' «humain». L'amélioration constante des politiques de sécurité de l'information, la formation et la sensibilisation auprès des employés et des exécutifs ainsi que la cohérence des actions entre les intervenants ne sont que quelques-uns des moyens pour permettre ne serait-ce qu'une réduction des risques informationnels.

2.3.4 La protection du patrimoine informationnel de l'entreprise

Devant un éventail aussi large de risques, le gestionnaire doit «mettre en place des dispositifs et dispositions de protection» (Vuillerme 2010, p.63) pour s'assurer que l'information soit sécurisée de façon efficace et efficiente. La définition de la sécurité de l'information élaborée par Lessard reflète la réalité actuelle des organisations qui concèdent de plus en plus que l'information ne se limite pas nécessairement aux systèmes et s'étend à tous les supports qu'ils soient virtuels ou physiques.

> «La sécurité de l'information, c'est l'ensemble des activités qui préservent la disponibilité, l'intégrité et la confidentialité de l'information et ce, peu importe le support utilisé pour la conserver ou la transmettre. C'est aussi un ensemble de mesure de sécurité pour assurer l'authentification des personnes et des dispositifs ainsi que l'irrévocabilité des actions qu'ils posent» (Lessard 2009, p.2).

Loin de prétendre que les mécanismes de protection sont à toute épreuve, ceux-ci permettent néanmoins d'établir un cadre où seront mises en commun les meilleures pratiques. La sécurité de l'information demeure un objectif, un idéal théorique à atteindre et si la sécurité absolue n'existe pas, certains critères de base doivent être respectés. Ces principaux critères se résument à la confidentialité, l'intégrité, la disponibilité et la traçabilité (von Solms 2001; Posthumus & von Solms 2004; FISMA[9] 2004; Livre Blanc CIGREF 2007; Lessard 2009).

[9] Federal Information Security Management Act.

- La confidentialité : il s'agit de s'assurer que le patrimoine informationnel de l'entreprise demeure protégé contre toute intrusion. L'information confidentielle doit demeurer confidentielle;
- L'intégrité : préserver l'intégrité de l'information consiste à en maintenir «l'exactitude et l'exhaustivité» (Posthumus & von Solms 2004, p.640). Autrement dit, s'assurer que l'information n'est pas, en partie détruite ou altérée;
- La disponibilité : l'information doit être accessible en temps voulu par les personnes autorisées à en faire usage;
- La traçabilité : chaque donnée laisse une «empreinte» de son cheminement, à partir de sa production jusqu'à sa destruction.

Dans la mesure où l'un de ces quatre critères pourrait être compromis par un acte malveillant, de la négligence, de l'incompétence ou parce que les mesures de sécurité sont inadéquates, le gestionnaire doit procéder à une analyse de l'impact que cette brèche sécuritaire pourrait occasionner à l'entreprise. Dans le cadre de cette recherche, nous nous baserons sur la formulation donnée par la *National Institute of Standards and Technology* qui utilise le processus de standardisation de la FIPS (Federal Information Processing Standard)[10] pour décrire trois niveaux d'impact potentiel pouvant affecter la confidentialité, l'intégrité, la disponibilité et la traçabilité de l'information. L'impact est considéré comme faible si la perte de confidentialité, d'intégralité et de disponibilité a un effet limité sur les opérations de l'organisation et son patrimoine informationnel. L'impact est modéré lorsque l'effet sur les opérations de l'organisation et son patrimoine informationnel est sérieux mais ne menace pas sa survie. Finalement, l'impact est considéré comme élevé lorsque la perte de confidentialité, d'intégralité et de disponibilité a un effet si sévère que les activités de l'organisation pourraient être interrompues de manière définitive (FISMA 2004). Une fois l'impact potentiel établi, s'ensuit une catégorisation de l'information et un ajustement quant au niveau de sécurité qui doit être appliqué à chacune de ces catégories. Cette catégorisation n'est pas systématique dans toutes les entreprises et les critères ne sont pas toujours respectés

[10] Standards publiés par le gouvernement fédéral américain quant à l'utilisation des systèmes d'information par des organismes ou entreprises privées sous contrat avec le gouvernement.

intégralement. Cela s'explique principalement par le fait que non seulement la sécurité de l'information suppose l'utilisation de moyens technologiques et humains qui varient ostensiblement d'une entreprise à une autre mais aussi que chaque entreprise ne bénéficie pas nécessairement d'un service ou département dédié spécifiquement à la sécurité de l'information.

Certes, la sécurité de l'information n'est plus uniquement l'affaire d'informaticiens ou d'ingénieurs chevronnés voués à maintenir une architecture des systèmes d'informations à l'épreuve des défaillances techniques ou des intrusions inopportunes (Posthumus & von Solms 2004). Elle nécessite également la mise en place de processus organisationnels formels dont la responsabilité incombe au gestionnaire de la sécurité ou de la sécurité de l'information (COSO 2005; Ebondo Wa Mandzila & Zéghal 2009; Beldjilali 2009; Lessard 2009; Steinbart & al. 2012). Dans la plupart des organisations, trois fonctions sont impliquées de façon directe et concrète dans la sécurité de l'information; la fonction «sécurité des systèmes d'informations», la fonction «sécurité physique» et la fonction «audit»[11] (Steinbart & al. 2012). Dans le cadre de cette recherche, nous nous intéresserons plus particulièrement aux deux premières puisque la troisième est plus fréquemment offerte en sous-traitance comme c'est le cas dans bien des PME.

2.4 Le gestionnaire de la sécurité dans l'entreprise

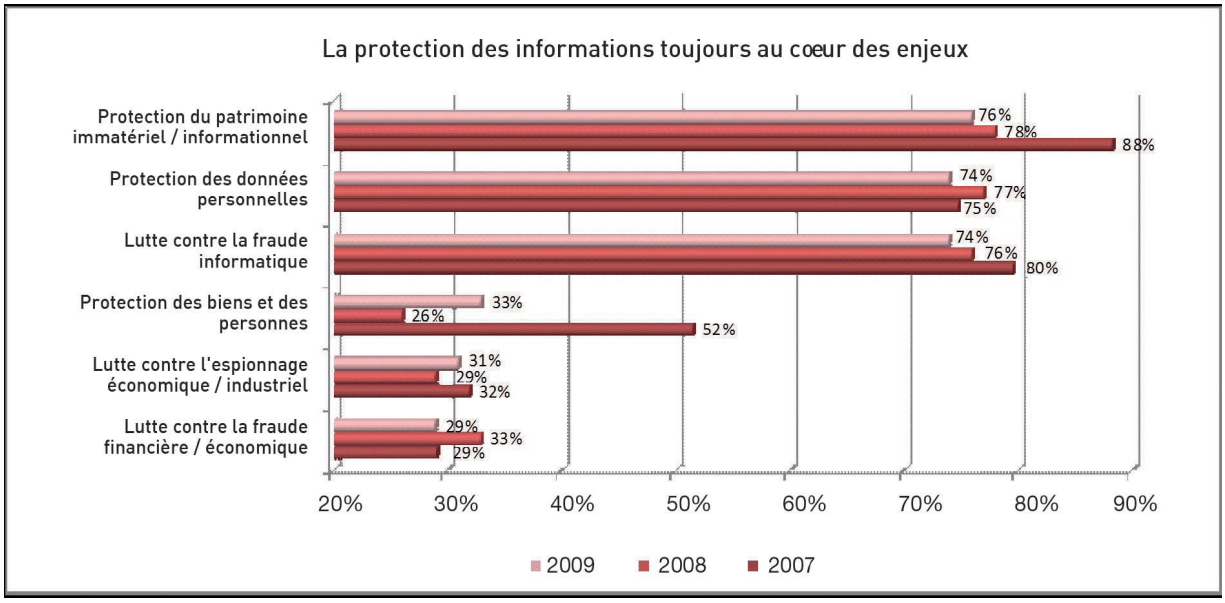
2.4.1 Rôles et responsabilités des gestionnaires de la sécurité en matière de gestion des risques informationnels

Comme nous l'avons mentionné plutôt, un gestionnaire fait face à quatre principales options en matière de gestion des risques informationnels: l'inaction ou l'acceptation, la

[11] La sécurité des systèmes d'information fait surtout référence à la sécurité des données, du réseau et de l'architecture du système. La sécurité physique réfère principalement à la sécurité des biens, des personnes et des lieux. Quant à la fonction audit, il s'agit du processus de vérification et de respect des normes.

réduction, l'évitement, le transfert à une tierce partie ou l'abandon (Button 2008; Ebondo Wa Manzilla & Zéghal 2009; Dupont 2010). Le choix d'une option dépend de plusieurs facteurs, notamment de sa connaissance des risques passés, actuels et potentiels, de sa connaissance du contexte organisationnel, de la qualité de l'information qui lui parvient (fiable, pertinente, récente et complète), du système de communication (mécanismes de communication formels et informels) et de la culture informationnelle qui prévaut au sein de son entreprise (Ebondo Wa Manzilla & Zéghal 2009). Le secteur d'activités de l'entreprise, l'étendue de son marché mais aussi, la fonction que le gestionnaire occupe, détermineront en partie son rôle et ses responsabilités en matière de gestion des risques informationnels. Le *Livre Bleu des Assises de la Sécurité et des Systèmes d'Information*[12] publie chaque année depuis 2004, l'état de la situation relative à l'évolution des «activités et des rôles des professionnels de la sécurité des systèmes d'information». Le sondage réalisé en 2009 auprès de 240 de leurs membres est révélateur des préoccupations des professionnels de la sécurité de l'information puisque la protection du patrimoine informationnel figure en tête de liste des domaines d'action des professionnels de la sécurité.

Tableau 3. Domaines d'action des professionnels de la sécurité de l'information.



Tiré du Livre Bleu des Assises de la Sécurité et des Systèmes d'Information

[12] Le cercle européen de la sécurité et des systèmes d'information. Octobre 2009.

Notons ici que ce tableau ne distingue pas le domaine d'expertise du professionnel de la sécurité de l'information, ce qui nous aurait permis de mettre en perspective les domaines d'action privilégiés pour chaque type de professionnel. Nous savons seulement que le panel est composé de directeurs de la sécurité physique, de directeurs de la sécurité informatique, de gestionnaires de risques, de responsables de la sécurité de l'information et de responsables de la sécurité informatique. Précisons également que la proportion d'acteurs internationaux est de 31%.

Il en va de même pour les études internationales portant la sécurité de l'information, réalisées par des firmes spécialisées telles que Deloitte, Ernst & Young et PricewaterhouseCoopers. Les questionnaires et/ou les entrevues sont réalisés auprès du gestionnaire principal de la sécurité (chief of security) ou du CISO (Chief information security officer) dans le cas de Deloitte. PricewaterhouseCoopers et Ernst & Young dans leurs rapports annuels sur la sécurité de l'information interrogent quant à eux des gestionnaires de tous les niveaux, du CEO (Chief executive officer) au directeur de la sécurité de l'information en passant par le vice-président TI. Dans la compilation des données, il n'y a pas de distinction quant au champ d'expertise ou quant à la fonction des participants.

Nous pouvons cependant remarquer que la sécurité de l'information et par extension, la gestion des risques informationnel, est assurés par des professionnels de la sécurité issus principalement de trois domaines d'expertise différents (finance, informatique, sécurité). Leur position dans la structure hiérarchique varie également d'une entreprise à une autre. Fort est de constater que dans les très grandes entreprises, il est fréquent de trouver un gestionnaire de la sécurité globale chapeautant la sécurité physique et la sécurité informatique. Dans d'autres organisations, petites ou moyennes, cette responsabilité peut relever d'un gestionnaire TI (comme c'est le cas pour 63% des entreprises sondée par Ernst & Young en 2012) ou d'un gestionnaire de la sécurité physique. Plusieurs organisations ont également un comité de gouvernance de la sécurité de l'information composé de gestionnaires qui ont le mandat d'élaborer les plans d'action et de formaliser

les processus de gestion des risques informationnels. Les modèles sont variés et parfois complexes alors qu'à d'autres occasions, ils sont quasi inexistants.

Ainsi, le gestionnaire à qui incombe la responsabilité de la sécurité de l'information et par conséquent, la gestion du risque informationnel fait face à des exigences similaires, peu importe le titre qu'il porte. Il doit prendre en considération une multitude de facteurs tant à l'interne qu'à l'externe pour identifier, hiérarchiser et enfin, contrôler les risques. Il doit également composer avec les objectifs de son propre département et s'assurer que ceux-ci s'harmonisent avec les objectifs de rentabilité de l'entreprise. Le gestionnaire de la sécurité[13] «tient compte d'un certain nombre de contraintes lorsqu'il effectue ses recommandations et il fait des compromis» (Fisher & Green 2004, p.138), notamment sur les coûts des mesures qu'il doit mettre en place (Mignault 2007). Si le rôle premier du gestionnaire de la sécurité est de veiller à la protection des actifs corporatifs, il doit aussi comprendre que «la survie de l'entreprise passe (…) par l'acceptation, par l'entreprise, d'une prise de risque» (Ebondo Wa Manzilla & Zéghal 2009, p.18). Autrement dit, l'approche traditionnelle d'une sécurité absolue et compartimentée ne trouve plus sa place au sein des organisations qui démontrent la volonté d'adopter une approche plus «intégrée» de gestion des risques informationnels.

Pour cette raison, le rôle du gestionnaire de la sécurité tend à évoluer et ses responsabilités se transforment au contact d'un environnement toujours changeant : les fonctions se décloisonnent et les responsabilités se chevauchent. La sécurité de l'information ne concerne plus uniquement l'unité responsable de l'architecture des systèmes tout comme la sécurité des actifs corporatifs n'est plus l'apanage exclusif du directeur de la sûreté. Il est d'autant plus difficile d'identifier spécifiquement les tâches effectuées par le gestionnaire responsable de la sécurité de l'information puisque celles-ci sont rarement circonscrites à l'intérieur d'un cadre précis et défini (Ocqueteau 2011). Généralement, elles peuvent se résumer ainsi :

[13] Dans un souci de préserver la clarté du texte, nous avons délibérément utilisé, dans ce chapitre, le terme «gestionnaire de la sécurité».

- assurer la direction de son département : gérer et former son personnel;
- réaliser des analyses de risque ponctuelles;
- élaborer et mettre en œuvre des politiques de sécurité;
- participer à l'élaboration de plans de relève et de mesures d'urgence;
- s'informer périodiquement des incidents touchant de près ou de loin la sécurité de l'information à l'aide d'outils statistiques;
- mettre en place une veille sur les menaces et vulnérabilités;
- élaborer les politiques relatives à la confidentialité, l'intégrité, la disponibilité et la traçabilité de l'information;
- favoriser l'intégration des politiques de sécurité de l'information à tous les niveaux de l'organisation;
- s'assurer que l'entreprise respecte les normes et standards de l'industrie en matière de sécurité de l'information;
- faire en sorte que l'entreprise respecte les lois et règlements en vigueur;
- assurer la coordination et la cohérence des actions entre son département et les autres unités;
- siéger sur des comités sectoriels, participer à des conférences;
- favoriser la formation continue pour ses subalternes et pour lui-même;
- recommander la mise en place de nouveaux processus ou proposer des changements afin d'améliorer les processus existants.

Évidemment, les responsabilités du gestionnaire diffèrent considérablement d'une entreprise à une autre. Outre la structure et la taille de l'entreprise, la nature de ses activités détermine aussi, en partie, les tâches qu'aura à accomplir le gestionnaire de la sécurité. L'exploitation des ressources naturelles, de l'énergie nucléaire ou encore, le développement de nouvelles technologies ne nécessitent pas les mêmes mesures que la sécurité dans le commerce au détail, par exemple. À cette liste non exhaustive, faut-il le souligner, un nombre important de tâches connexes viendront s'ajouter ou se soustraire au gré des projets auxquels le gestionnaire participera au cours de son mandat.

2.4.2 Caractéristiques personnelles du gestionnaire

Face à des responsabilités aussi diverses que multiples, le savoir dont le gestionnaire dispose se révèle essentiel à chaque étape du processus décisionnel lié à la gestion du risque. «Organisational knowledge has long been recognised as a resource of strategic significance and the importance of knowledge management is now well established» (Shedden & al. 2002, p.154). Non seulement ce savoir doit incorporer les connaissances qu'il a de son environnement externe mais il doit aussi être en mesure de bien comprendre l'environnement interne de l'entreprise : sa structure, ses objectifs stratégiques, son processus d'affaires et ses mécanismes relationnels (Shedden & al. 2002; Berg & Shearing 2008; SANS Institute 2009; Ocqueteau 2011). Le savoir organisationnel, c'est aussi l'expérience du gestionnaire et sa compétence dans divers domaines d'activités (Davenport & Prusak 1998; Ashenden 2008). Davenport et Prusak (1998) distinguent deux formes de connaissances : la connaissance explicite qui se traduit par un langage formel et structuré (une politique de sécurité par exemple) et la connaissance tacite, qui fait référence au savoir-faire et à l'expérience de l'individu.

Une gestion des risques informationnels efficace suppose également que le gestionnaire possède d'excellentes habiletés communicationnelles (Ashenden 2008; Ebondo Wa Manzilla & Zéghal 2009; SANS Institute 2009; Ocqueteau 2011). La SANS Institute insiste d'ailleurs sur ce point: «Developing strong people skills should not be underestimated» (2009 p.3). Les résultats de l'étude réalisée par Ocqueteau en 2011 vont dans le même sens et nous montrent que les gestionnaires de la sécurité seraient recherchés pour leur «capacités de dialogue social» (Ocqueteau 2011, p.44). Savoir convaincre et avoir la capacité d'influencer se révèlent être des plus-values pour le gestionnaire; autant lorsqu'il est question de sensibilisation auprès des employés que lorsqu'il est question de négocier l'attribution d'un budget pour un nouveau projet (Mulone & Desroches 2011). Cette capacité d'influencer et de communiquer le risque ne doit pas provenir du fait que le gestionnaire soit titulaire d'une autorité formelle mais plutôt parce que les employés lui font confiance et croient en son interprétation des problèmes (SANS Institute 2009; Ocqueteau 2011). Il s'agit donc, pour le gestionnaire,

d'établir un équilibre entre ses compétences techniques, ses compétences relationnelles et ses habiletés communicationnelles. Ces qualités constituent des atouts considérables pour faciliter l'intégration de nouvelles politiques ou encore pour développer des relations auprès de futurs partenaires.

2.4.3 La pluralité des acteurs : réseaux

Par ailleurs, que nous parlions de la nature de ses activités, de la taille de son marché, de ses ressources financières et humaines, de son stade de développement ou de la culture informationnelle véhiculée par ses dirigeants, la structure organisationnelle d'une entreprise est aussi variée que la multitude d'acteurs qu'y viennent s'y greffer de façon permanente ou provisoire. En matière de gestion des risques informationnels, le gestionnaire de la sécurité n'échappe pas à cette dynamique. Afin de mener à bien le projet sécuritaire qui lui incombe, il doit tisser des liens avec divers acteurs qui se révèlent parfois utiles lorsqu'il s'agit par exemple de discuter de questions sécuritaires ou de tendances en matière de criminalité en entreprise.

Cette dynamique implique nécessairement l'organisation de groupes formels et informels et cela, tant à l'externe qu'au sein même de l'organisation. «Le groupe formel est un groupe officiellement désigné pour assumer un rôle précis au sein d'une organisation» (Schermerhorn & al. 2010, p.219). Les unités départementales, les comités de travail et les divisions en sont de bons exemples. Ces groupes peuvent être provisoires ou permanents. Il peut aussi s'agir de groupes d'études ou d'équipes dédiées à la réalisation de projets spéciaux. Les groupes informels quant à eux «se forment spontanément, au gré des relations personnelles ou pour répondre à certains domaines d'intérêts communs de leurs membres sans l'intervention ou l'appui officielle de l'organisation» (Schermerhorn & al. 2010, p.221). Ces groupes sont autonomes et indépendants et la participation de leurs membres est libre et volontaire. Nous comptons parmi ces groupes informels les associations professionnelles, les communautés virtuelles (Facebook, Linkedin), les comités sectoriels et les groupes de discussions pour ne nommer que ceux-là.

Les réseaux de sécurité pourraient faire partie du premier ou du deuxième groupe puisque «…les réseaux de sécurité sont en fait le résultat de relations bilatérales et multilatérales multiples qui s'agrègent autour de pratiques et d'enjeux communs pour définir un champ organisationnel différencié : celui de la sécurité» (Dupont 2006 p.349). Ces groupes organisés ou plutôt «connectés» en vue «d'améliorer leur efficacité et de réduire leur vulnérabilité aux risques et aux contingences extérieures» (Dupont 2006, p.350-351) favorisent la communication et l'échange d'informations et trouvent leur utilité principalement lorsqu'il est question de lutte à la criminalité (perte ou vol de données) (Dupont 2006; Gauthier-Gaillard & Faucon 2010). Les réseaux de sécurité contribuent également à faciliter la gestion des risques informationnels et jouent un rôle essentiel à certaines étapes du processus décisionnel notamment à l'étape de la reconnaissance des risques ainsi que lorsqu'il est question de solutionner un problème récurrent dans un secteur en particulier (Dupont 2006; Gauthier-Gaillard & Faucon 2010).

Les mécanismes de cette transmission de l'information s'apparentent au système de communication du risque décrite par Erickson et Haggerty (1997). Leur thèse, élaborée à partir d'une étude empirique du milieu policier suppose non seulement que les policiers sont les producteurs d'un savoir sur le risque mais qu'ils aussi les promoteurs de ce même risque. Le partage des connaissances et la diffusion du risque impliquent, dans un cas comme dans l'autre (au privé ou au public), un processus qui transcende l'organisation et qui profite à un cercle élargi d'acteurs. À ce sujet, Ocqueteau (2011) précise que «la nécessité est reconnue par tous de multiplier et systématiser les échanges informels sur les expériences préexistantes dans les cercles dédiés à cet effet (...)» (p.51). Comme nous l'avons souligné à maintes reprises, l'efficacité d'un processus de gestion des risques informationnels repose d'abord sur une connaissance approfondie de l'environnement interne et externe de l'entreprise et sur la maîtrise de l'information qui circule au sein de cet environnement. C'est dans cette perspective que le réseau contribue au processus décisionnel du gestionnaire en matière de gestion des risques informationnels. C'est pourquoi, dans le cadre de cette recherche, il nous faudra aussi

tenir compte de la dimension relationnelle de la production de sécurité et de la gestion des risques informationnels.

2.4.4 Collaboration, négociation et synergie

À l'interne, si quelques acteurs centraux exercent une influence sur le processus décisionnel du gestionnaire de la sécurité, ils contribuent aussi à augmenter le degré de difficulté de gestion. «Certains tiers (…) fournissent fréquemment des informations utiles au dispositif de management des risques, mais ils ne sont pas responsables de son efficacité et ne participent pas à sa mise en œuvre» (COSO 2005). Prenons par exemple le conseil d'administration «(…) qui exerce une activité de surveillance sur le dispositif de management des risques, il a connaissance et valide l'appétence pour le risque de l'organisation» (Ebondo Wa Mandzila & Zéghal 2009). Notons aussi les activités d'audit qui servent à produire des rapports périodiques visant principalement à évaluer l'efficacité des mesures de contrôle en place, à renseigner le gestionnaire au sujet des points à améliorer et le cas échéant, à proposer des correctifs (Steinbard & al. 2012). Mentionnons finalement la direction des finances qui octroie les budgets ou la direction des affaires juridiques qui doit s'assurer que les projets respectent les lois et règlements en vigueur. Et ce ne sont là que quelques uns des acteurs avec lesquels le gestionnaire doit traiter sur une base régulière ou sporadique. Encore une fois, ses habiletés communicationnelles et sa compréhension de la réalité organisationnelle lui seront fort utiles s'il souhaite préserver la qualité de ses relations professionnelles (Ashenden 2008; Schermerhorn & al. 2010; Ocqueteau 2011). Qui plus est, le gestionnaire aura à s'engager dans diverses stratégies de négociation avec certains acteurs clés de l'organisation car le pari d'atteindre un «équilibre optimal» entre la logique de sécurité et les «logiques concurrentes de rentabilité, de compétitivité ou encore de qualité du service offert à la clientèle» (Dupont, 2010, p.8) pourra être gagné si «la conciliation des intérêts respectifs» (Schermerhorn & al. 2010, p.429) est prise en considération.

Par ailleurs, certains groupes sont créés précisément avec l'intention de faire participer des tiers dans le processus décisionnel lié à la gestion des risques informationnels. Ces groupes se retrouvent à la fois dans la petite entreprise où le propriétaire-gestionnaire est directement impliqué dans la prise de décision et dans la grande entreprise puisque le groupe permet de «remédier aux inconvénients liés à la grande taille d'une organisation» (Schermerhorn & al. 2010). Ces groupes, composés majoritairement de cadres, permettent de définir les priorités en termes de risques, d'établir les mandats et d'élaborer des plans stratégiques en liens avec les objectifs de l'entreprise. Plusieurs auteurs s'entendent pour dire que malgré les nombreux avantages liés à l'utilisation de groupe de travail ou de comité de direction, l'approche participative peut amener son lot de difficultés (Ashenden 2008; Forte 2009; Steinbart & al. 2012). Dans une structure où les responsabilités se chevauchent et où le leadership est informel, le succès du projet dépendra principalement de la synergie et de la collaboration entre les membres du groupe (Ashenden 2008).

Au regard de ce qui précède, nous constatons que l'ampleur et la complexité du travail qui incombe au gestionnaire de la sécurité en matière de gestion des risques informationnels est tributaire de plusieurs facteurs d'ordre contextuel, relationnel et personnel. La globalisation des marchés, la pluralité des acteurs et surtout, le développement effréné des technologies de l'information exercent une influence sur la prise de décisions relative à la gestion des risques informationnels. «Les membres d'une organisation - peu importe sa taille, son type et son champ d'activité - doivent faire bien plus que prendre des décisions (…) ils doivent prendre les bonnes décisions, de la bonne manière et au bon moment» (Schermerhorn & al. 2010, p.375). Comme plusieurs gestionnaires de la sécurité occupent désormais des positions dites stratégiques au sein de leur organisation, il devient nécessaire de faire le point sur la place qu'occupe la sécurité de l'information dans l'exercice de leurs fonctions. De même, nous devons considérer la possibilité que de nouveaux enjeux, notamment sur le plan technologique, influencent la gestion des risques et par le fait même, complexifient la protection du patrimoine informationnel de l'entreprise.

2.5 Cadre théorique

D'un point de vue théorique, l'entreprise est une organisation où un «regroupement d'individus (…) qui travaillent à un objectif commun, à savoir, la production de biens ou de services pour la société» (Schermerhorn et al. 2010, p.10). Nous avons vu que la gestion des risques informationnels dans l'entreprise, est issue d'un processus organisationnel qui dépend d'une multitude de facteurs tant humains, financiers, technologiques que légaux pour ne nommer que ceux-là. Une partie de ce processus est formalisé par la mise en place de procédures et de normes internes et externes. La seconde partie du processus de gestion des risques informationnels nous renvoie davantage à des mécanismes informels à travers lesquels s'imbriquent les conduites individuelles et sociales des acteurs impliqués.

Ce système complexe de règles et de relations formelles et informelles implique des acteurs qui doivent continuellement s'adapter à leur environnement. Non seulement ceux-ci doivent tenir compte des objectifs de l'entreprise et de leur position particulière au sein de cette dernière, mais ils ont aussi à composer avec leurs propres motivations personnelles (Thuderoz 2010; Schermerhorn et al. 2010; Foudriat 2011). Pour être en mesure de bien saisir la réalité des acteurs de la sécurité dans l'entreprise privée, il importe donc d'appréhender sociologiquement l'entreprise «comme un lieu de pratiques sociales, un espace abritant des relations sociales, des jeux et des règles» (Thuderoz 2010, p.5). L'entreprise doit aussi être considérée comme un lieu où les échanges sont issus de négociations perpétuelles entre les acteurs. Le gestionnaire de la sécurité se retrouve donc face à deux réalités organisationnelles : l'aspect contextuel lié à la sécurité de l'information et l'aspect relationnel de la gestion. Ces deux aspects viennent influencer, à divers niveaux, l'information qui parvient au gestionnaire de même que sa façon d'apprécier le risque et d'en gérer les tenants et aboutissants. Dans le cadre de cette recherche, deux approches seront utilisées pour rendre compte du processus décisionnel de la gestion des risques informationnels : l'approche de la transaction

sociale (pour l'aspect relationnel) et l'approche multidimensionnelle du risque de Kermisch (pour l'aspect contextuel).

L'approche de la transaction sociale relève d'une discipline relativement nouvelle qui fut conceptualisée vers la fin des années 70 par Jean Rémy (1978). Elle «emprunte à l'économie (…) et au droit (…) et le contexte d'incertitude de la «société du risque» (Beck, 2001) a fait en sortes d'élargir la portée de cette approche à travers différents objets d'études comme la prévention de la délinquance (Nécol 2005), la gestion des risques industriels (Gibout & Zwarterook, 2013) et la gouvernance territoriale des risques technologiques (Le Blanc et al. 2013). «La transaction sociale intervient dans la construction sociale des compromis qui organisent, par exemple, la gestion des risques et des incertitudes» (Foucart et al. 2013, p.10). Parce qu'elle se traduit par une dynamique d'échange et de négociation entre les acteurs, cette approche nous semble la plus appropriée pour analyser le processus décisionnel des gestionnaires de la sécurité d'un point de vue relationnel. Dans le cadre de cette recherche par exemple, nous considérerons l'entreprise comme un lieu social où les acteurs impliqués dans la gestion des risques informationnels doivent quotidiennement s'ajuster en fonction des problèmes à résoudre. Ils doivent prendre position et négocier quant aux solutions qui seront adoptées. En tenant compte de ces éléments, nous nous demanderons ainsi comment s'effectue la gestion des risques informationnels dans un contexte organisationnel où les logiques sécuritaires sont parfois en conflits avec les logiques d'affaires.

Il faut retenir que la transaction sociale «ne présuppose pas que l'accord découle de procédures rationnelles et clairement formalisées. Elle est attentive aux accords informels, implicites ou tacites» (Blanc 2009, p.131) mais demeure fondamentalement une «interaction cadrée» (Rémy 2005, p.93). Il nous sera donc possible, à travers cette approche, de tenir compte de ce type d'accords, de ces «arrangements». Il est également essentiel de souligner que la transaction sociale «véhicule une vision complexe d'un acteur toujours situé, des forces qui le font agir (…) et de l'inextricable mélange des compétences dont il fait preuve» (Fusulier B. & N. Marquis 2008, p.20). Dans cette

perspective, il convient d'exploiter cette approche pour analyser les discours des gestionnaires tout en tenant compte de leur profil, de leur expérience et de leurs compétences. Et bien que cette approche comporte plusieurs similitudes avec l'analyse stratégique, théorie développée par Michel Crozier et Erhard Friedberg, la principale différence, selon Rémy (2005), réside dans les motivations de l'acteur, c'est-à-dire qu'il ne considère pas que le jeu des acteurs se réduit à un calcul stratégique. Dans l'analyse d'une dynamique organisationnelle, l'approche de la transaction sociale ne nie pas les divergences d'intérêts ou la présence de stratégie individuelle (Rémy 2005; Thuderoz 2010; Schermerhorn et al. 2010; Foudriat 2011). Elle reconnait cependant que la dynamique de l'échange est complexifiée par une multitude de variables et de dimensions qui ne sont pris en compte que superficiellement dans la théorie de l'acteur stratégique. La transaction sociale n'étant pas une théorie en soi mais plutôt une approche, elle invite le chercheur à pratiquer «l'hybridation de théories et des disciplines» (Foucart et al. p.14). De fait, il est possible de l'articuler avec d'autres approches, notamment, certaines théories issues de la sociologie du risque (Blanc 2009).

Il faut toutefois être prudent relativement à la manière de traiter le risque et plus particulièrement le risque informationnel en entreprise puisque celui-ci est traditionnellement mesuré à l'aide de modèles d'analyse de risques automatisés. Plusieurs recherches démontrent cependant que la gestion des risques informationnels ne peut s'accomplir uniquement qu'à partir de mesures quantitatives (Bulinge 2002; Tsoumas & Tryfonas 2004; Shedden & al. 2011; Kermisch 2012). L'analyse de risque résulterait aussi d'une évaluation qualitative faite par le gestionnaire et qui tiendrait compte de différents facteurs dont l'expérience et les connaissances dont il dispose, de l'information qui lui parvient, de la culture informationnelle de l'entreprise, de la position qu'il occupe au sein du modèle de gouvernance de l'entreprise ainsi que des contraintes et opportunités qui s'offrent à lui. L'approche multidimensionnelle du risque élaborée par Kermisch (2012) s'applique au processus décisionnel du gestionnaire parce qu'elle tient compte d'une multitude de dimensions et est «capable de concilier une composante quantitative (…) et une composante qualitative susceptible de rendre compte d'enjeux éthiques, politiques, sociétaux, etc., lesquels interviennent dans l'évaluation et

la gestion du risque» (Kermisch 2012, par. 46). L'auteur insiste d'ailleurs sur une conception du risque «ouverte et contextuelle» où certains facteurs organisationnels comme l'engagement, les compétences et les connaissances trouvent leur place au sein d'un modèle de gestion des risques. Ainsi, notre hypothèse soutient que le gestionnaire de la sécurité se sert de ce qui s'apparente à une approche multidimensionnelle des risques dans sa gestion des risques informationnels. L'exercice consiste donc à utiliser les principes de cette approche pour illustrer de quelle façon le gestionnaire de la sécurité concilie les dimensions qualitative et quantitative dans sa conception du risque informationnel. La transaction sociale permet finalement d'intégrer à ce cadre, la dimension relationnelle, fondamentale au processus décisionnel de gestion des risques informationnels.

Il s'agit donc d'analyser un processus dynamique qui, loin d'être statique, suppose trois aspects qui ne sont ni distincts, ni interdépendants : l'aspect contextuel, l'aspect relationnel et l'aspect individuel ou le profil du gestionnaire de la sécurité. Parce que les risques changent autant que le contexte organisationnel évolue, chaque aspect entre en jeu à un moment indéterminé du processus décisionnel de gestion des risques.

> «En définitive, chaque cas de figure, chaque nouvelle technologie, chaque nouvelle substance, chaque nouvelle activité à risques, ou chaque nouveau contexte, impose une analyse nouvelle afin de dégager les valeurs et critères qualitatifs qui exigent leur intégration à la définition du risque.» (Kermish 2012, par.46)

Il n'est donc pas question de prétendre pouvoir tracer ou définir un modèle particulier de gestion des risques informationnels. Il s'agit davantage de comprendre en quoi consiste ce processus décisionnel, de savoir ce qui vient l'influencer et par conséquent, de mieux situer le gestionnaire de la sécurité, définir son cadre d'action, ses tâches et ses responsabilités au sein de l'organisation.

2.5.1 Problématique et objectifs de recherche

La littérature nous offre une quantité non négligeable d'informations traitant de la gestion du risque ou de la sécurité de l'information. Les études empiriques portant spécifiquement sur la gestion des risques informationnels dans le secteur privé se font cependant plus rares. Les enquêtes annuelles de certaines firmes comme PricewaterhouseCoopers et Deloitte nous offrent par ailleurs un portrait intéressant de la situation puisqu'elles rendent compte de l'évolution des mentalités et de la prise de conscience des enjeux relativement à la sécurité de l'information. En 2009 par exemple, les conséquences de la crise économique se sont fait ressentir à travers l'industrie. La fonction «sécurité» a essuyé un important revers, notamment au niveau des budgets qui pouvaient lui être consacrés. 70% des répondants interrogés par la firme PWC (rapport annuel de 2009) rapportent qu'une partie de leur budget de sécurité a été transféré ou diminué pour compenser des besoins opérationnels ou des besoins en capital. En 2010 et 2011, on réitère l'importance de privilégier la sécurité de l'information au sein des organisations mais la tâche semble ardue et cela, malgré des risques qui se matérialisent à plusieurs reprises par le biais de cyber attaques ou d'espionnage industriel. En 2012 et en 2013, la sécurité de l'information devient un objectif prioritaire, les organisations sont davantage proactives et les gestionnaires de la sécurité de l'information bénéficient d'un meilleur support de la direction. En effet, l'étude de PWC révèle que 45% des répondants prévoyaient, dans les douze mois à venir, une augmentation de leur budget dédié à la sécurité de l'information.

Toutefois, certains problèmes subsistent: «…most organizations in the survey are challenged with balancing the cost of information security initiatives with the perceived risks of sophisticated threats and emerging technologies» (Deloitte 2012, p.3). Qui plus est, l'obtention d'une enveloppe budgétaire suffisante pour parer à une quantité toujours grandissante de risques informationnels fait encore l'objet de négociations, de jeux de pouvoir et de stratégies relationnelles. Et si, par le biais d'enquêtes, nous disposons de statistiques qui nous informent sur les tendances générales de l'industrie de la sécurité de

l'information, les résultats demeurent difficilement contextualisables et les mécanismes relationnels restent, quant à eux, largement inconnus.

C'est en tenant compte de cette réalité que nous avons élaboré les objectifs de cette recherche. Notre objectif principal consiste donc à comprendre, à partir de la perspective des responsables de la sécurité, comment s'effectue la gestion des risques informationnels dans une entreprise privée. Notre compréhension de la gestion des risques de même que notre appréhension du discours des responsables de la sécurité passent nécessairement par une connaissance approfondie du contexte organisationnel et des principes relationnels qui en émergent. C'est en considérant ces facteurs que nous avons défini les objectifs spécifiques suivants :

- comprendre le processus d'identification et de hiérarchisation des risques lorsqu'il est question de la protection du patrimoine informationnel;
- connaitre les dynamiques qui existent entre les acteurs internes et externes qui interviennent dans ce processus;
- comprendre le rôle du responsable de la sécurité en matière de gestion des risques informationnels et ce, à chaque étape du processus : de l'identification du risque à la mise en application des mesures de sécurité.

La réalisation des deux premiers objectifs nous permettra de comprendre comment s'effectue la gestion des risques informationnels en entreprise. Il sera aussi possible, par la réalisation du troisième objectif, de situer les gestionnaires de la sécurité au sein de ce processus et d'évaluer comment considérer que leur rôle et leurs responsabilités se sont transformés au contact d'une technologie en constante évolution et d'une globalisation des marchés qui complexifie les dimensions politiques, économiques et légales de la sécurité de l'information. Compte tenu de nos objectifs, l'élaboration d'un cadre théorique particulier combinant l'approche multidimensionnelle du risque et l'approche de la transaction sociale s'est avéré incontournable. De même, il nous fallait aborder notre sujet de recherche en considérant que la compréhension d'un processus décisionnel

passe nécessairement par une analyse des fondements d'une décision : quels sont les enjeux, les contraintes ou les opportunités qui s'imposent au gestionnaire de la sécurité? De quoi est composé le contexte? Qui intervient dans le processus et finalement, quel est le profil d'un gestionnaire de la sécurité?

CHAPITRE 3. MÉTHODOLOGIE

3. Méthodologie

3.1 La méthode qualitative

Comme nous venons de le souligner, l'objectif principal de ce mémoire consiste à connaître les pratiques de gestion des risques informationnels au sein d'entreprises privées. Dans la mesure où le risque (et sa gestion) est appréhendé à la fois comme un fait objectif et mesurable, et à la fois comme le résultat d'une construction sociale (c'est-à-dire comportant à la fois une dimension objective et une dimension subjective), il fallait être en mesure de bien saisir les enjeux liés à la gestion des risques informationnels et de comprendre le rôle du responsable de la sécurité dans la gouvernance de la sécurité de l'entreprise. Pour atteindre cet objectif, nous avons élaboré une approche qui mettrait l'emphase sur la façon dont le gestionnaire de la sécurité en arrive à adopter certains comportements ou certaines attitudes managériales relativement au risque. Revenons brièvement sur les éléments susceptibles de rendre compte de ce processus: l'aspect contextuel, l'aspect relationnel et le profil du gestionnaire de la sécurité, son rôle et ses responsabilités en termes de gestion des risques informationnels.

Ce «modèle» suggère que l'acteur, gestionnaire de la sécurité, adopterait une approche «multidimensionnelle du risque» (Kermish, 2012) : quantitative (analytique et historique) et qualitative (constructiviste). L'identification d'un risque et par conséquent, sa hiérarchisation seraient le résultat d'un mécanisme dynamique impliquant une multitude de sources (quantitatives et qualitatives) et d'interactions entre les acteurs (Gilbert 2003; Kermish 2012). Cette construction du risque contribuerait ensuite à façonner les décisions du gestionnaire de la sécurité et par le fait même à transformer le modèle de gouvernance de l'entreprise en matière de sécurité de l'information. La complexité de ce processus serait difficilement appréciable à travers les méthodes quantitatives puisqu'il existe, au sein de chaque entreprise, une culture organisationnelle et un mode de fonctionnement particulier qui se doit d'être saisie à partir d'une approche compréhensive (Van Maanen 1983). Van Maanen ajoute que peu importe le type

d'organisation, «we are certain to uncover special languages, unique and peculiar problems and, more generally, distinct patterns of thought and action» (Van Maanen, 1983, p.13). La méthodologie qualitative nous offre donc cette possibilité d'aller plus loin, de saisir le processus d'action de l'intérieur et d'en capter toute la substance. «Marchall et Rosseman soulignent d'ailleurs l'utilité et la supériorité méthodologique de la recherche qualitative, notamment lorsque cette recherche porte sur les processus organisationnels, leurs liens informels et non structurés» (Deslauriers et Kérisit 1997, p.86). Cette recherche étant élaborée autour d'un axe privilégiant la compréhension du processus décisionnel du gestionnaire de la sécurité au sein de son organisation, il paraissait approprié de privilégier une méthodologie qualitative.

3.1.1 Entretiens semi-directifs

Comme nous souhaitions approfondir nos connaissances au sujet de la gestion des risques informationnels dans l'entreprise privée à partir de la perspective des responsables de la sécurité, la méthode des entretiens semi-directifs paraissait toute indiquée (Ghiglione et Matalon 1998). Poupart souligne que «le recours aux entretiens demeure, en dépit de leurs limites, l'un des meilleurs moyens pour saisir le sens que les acteurs donnent à leurs conduites» (Poupart 1997, p.175). Au sujet des entretiens semi-directifs, Fenneteau ajoute que ce sont des méthodes «(…) souvent utilisées à titre principal pour réaliser des études qualitatives portant sur les perceptions et les attitudes des individus» (Fenneteau 2002, p.13). En ce qui concerne cette recherche, non seulement nous nous intéressons aux attitudes des individus à l'égard d'un sujet donné, mais nous devons aussi tenir compte de la réalité organisationnelle à laquelle ces individus sont confrontés.

Notre choix d'opter pour les entretiens semi-directifs s'explique aussi par le fait que nous souhaitons conserver la dimension spontanée et naturelle de l'échange et surtout, nous ne voulons pas nous soustraire au cadre de référence (langage, catégories mentales) du répondant en lui posant des questions trop fermées (Quivy et Van Campenhoudt,

1988). Nous avons donc procédé à des entretiens semi-directifs à partir d'un guide d'entretien dont les thèmes ont été élaborés en fonction des objectifs du projet (Fenneteau 2002) mais aussi en fonction du modèle d'analyse réalisé spécifiquement à cet effet.

3.1.2 Entretiens exploratoires

Avant d'entreprendre des entretiens semi-directifs formels, il était nécessaire de clarifier certains éléments de la problématique que nous souhaitions étudier. Pour ce faire, nous avons choisi de procéder à des entretiens exploratoires. Ces entretiens, plutôt informels et ouverts, ont «pour fonction de mettre en lumière certains aspects auxquels le chercheur n'aurait pas pensé spontanément de lui-même et à compléter ainsi les pistes de travail que ses lectures auront mis en évidence» (Quivy et Van Campenhoudt 1988, p.60). Comme il s'agit de se départir de tout présupposé ou préjugé, l'on se doit d'éviter de poser des questions trop dirigées ou empreintes de sous-entendus. Cette étape nécessite, par conséquent, de se préparer adéquatement. Nous avons donc procédé à trois entretiens dits «exploratoires». Le premier s'est déroulé alors que la question de recherche était encore floue alors que le second s'est tenu par téléphone, à un moment où les objectifs venaient de se concrétiser. Ces deux premiers entretiens se sont effectués auprès d'individus que nous pourrions qualifier «d'experts»[14]. Si le premier entretien a orienté notre question de recherche vers la gestion des risques, le second nous a permis de procéder à la diversification interne de notre échantillon.

Lors d'un entretien exploratoire, il faut aussi s'attendre à ce que la conversation nous entraîne vers un dénouement qui pourrait se traduire par une modification importante des objectifs de recherche. C'est d'ailleurs ce qui s'est passé dans le cas présent. Lors du troisième entretien, il a notamment été question de l'intérêt des entreprises pour ce type de recherche et de la collaboration qui nous serait permis d'anticiper de la part de celles-

[14] Un entretien a été mené auprès de deux responsables du SCRS. Le second (téléphonique) a été mené auprès d'un responsable d'un réseau d'entreprises de haute technologie. Quant au troisième, il a été réalisé auprès d'un expert (professeur et chercheur) en sciences de l'information.

ci. Bien qu'au départ, nous souhaitions construire notre échantillon à partir d'un bassin de PME, la personne rencontrée nous a fait part de la difficulté à joindre les gestionnaires de PME malgré l'aide et le support dont ils pourraient bénéficier: ce sont des gens qui n'ont pas de temps à consacrer à la recherche ou aux séances d'informations. Qui plus est, la plupart d'entres eux se sentent très peu concernés par les risques informationnels, laissant cette préoccupation aux multinationales. Ils n'ont, de ce fait, créé aucun poste relié précisément à cette responsabilité. À la suite de cet entretien, nous en sommes venus à la conclusion que non seulement il serait plus profitable d'élargir notre champ de diversification afin d'y inclure les moyennes et les grandes entreprises mais aussi, que nous devions nous entretenir tant avec les gestionnaires de la sécurité qu'avec les gestionnaires des systèmes d'information.

Notre choix de se tourner vers des experts durant la phase exploratoire s'explique par le fait que nous voulions que nos interlocuteurs possèdent une vision globale du phénomène. Nous souhaitions aussi qu'ils nous renseignent sur les particularités du terrain et qu'ils puissent contribuer à clarifier notre consigne initiale (Quivy et Van Campenhoudt 1988). En ce qui les concerne, la consigne a été la suivante: «En vous référant aux entreprises de votre secteur, que pouvez-vous me dire à propos de la façon dont s'effectue la gestion des risques liés à l'information stratégique?» À cette question, tous nous ont indiqué qu'une telle gestion est difficilement possible au sein des PME mais se voit de façon quasi systématique dans les grandes entreprises, peu importe le niveau de risque auquel elles sont confrontées.

3.2 Échantillonnage

C'est en tenant compte de ces informations que la stratégie d'échantillonnage s'est élaborée. L'échantillon a été constitué en fonction du secteur d'activité et de la taille des entreprises (nombre d'employés). Avec plus de 30 000 profils d'entreprises disponibles à travers plusieurs réseaux et sites gouvernementaux, il était essentiel d'organiser le

processus d'échantillonnage d'une façon particulièrement structurée. Nous avons donc procédé à un premier élagage des entreprises en tenant principalement compte de leur emplacement géographique. Furent priorisées les régions administratives suivantes : Outaouais, Laurentides, Laval, Montréal, Lanaudière, Montérégie, Estrie, Centre du Québec et Capital Nationale. Bien que nous souhaitions par la suite sélectionner des entreprises privées (de préférence des PME) qui, selon de nombreuses recherches (Nasheri 2005; Danielson 2009; Foryst 2010; Faucon & Gaultier-Gaillard 2010) constituent des sujets davantage enclins à adopter des pratiques de gestion des risques informationnels, trop peu d'entres elles (les PME) ont répondu à notre appel. Nous devions néanmoins considérer cette option ne serait-ce que pour la richesse d'informations que certains répondants auraient pu nous procurer (Patton 1990). Il faut cependant préciser que nous n'étions pas spécifiquement à la recherche de cas qui auraient soutenu la tendance véhiculée à travers la littérature. Au contraire, il aurait été particulièrement intéressant de rencontrer des cas où les pratiques de gestion des risques informationnels se seraient avérées absentes ou quasi-inexistantes et ce, malgré le fait que l'entreprise fasse l'objet de convoitise de la part de la concurrence (Silverman 2005).

La seconde étape consistait à identifier les entreprises qui disposent, au sein de leur structure organisationnelle, une fonction «sécurité». Plusieurs PME ont ainsi été exclues, de même que toutes les entreprises offrant leurs activités de sécurité en sous-traitance. Considérant ce qui précède, nous avons procédé à une première sélection. C'est à partir d'un bassin très restreint de 51 entreprises et en tenant compte des objectifs de la recherche que nous avons déterminé les critères d'échantillonnage. D'abord, précisons que nous avons procédé à un échantillonnage par cas multiples de micro-unités sociales sur la base du principe d'homogénéisation (Pires 1997). Afin de respecter les critères liés à l'homogénéisation et à la diversification interne, nous nous sommes, d'une part, limité aux entreprises privées. Les critères de diversification interne que nous avons choisis ont ensuite été déterminés en fonction du modèle conceptuel.

Notons que sur une proportion de 21 courriels envoyés à des PME, 21 courriels sont restés sans réponses. Nous avons également sollicité la collaboration d'ASIS, chapitre de

Montréal pour transmettre notre demande aux gestionnaires de la sécurité. Nous avons encore une fois essuyé un échec puisqu'une seule personne a répondu à notre demande. Ainsi, la plupart des participants ont été recruté à même mon réseau personnel de contact et comme la collecte de données ne progressait pas de façon satisfaisante vu le nombre particulièrement réduit de participants, une partie de l'échantillon a dû être constituée par la méthode «boule de neige». Quatre participants supplémentaires sont ainsi venus compléter notre échantillon.

Il est nécessaire de préciser que nous avions été mis en garde (lors des entretiens exploratoires) de la possibilité que très peu de gestionnaires de la sécurité acceptent de s'entretenir du risque lié à la protection de l'information. Le sujet est suffisamment sensible pour faire fuir plusieurs d'entre eux. Dans quelques cas, le département légal a même refusé que le gestionnaire accorde un entretien malgré les exigences de confidentialité qui encadrent le travail de recherche. Il faut aussi ajouter que la plupart des gestionnaires ont été particulièrement difficile à rejoindre étant donné leur horaire surchargé et leur niveau de responsabilité au sein de l'entreprise. Certains individus avaient acceptés l'invitation pour ensuite se désister en invoquant différentes raisons : l'entreprise faisait l'objet de poursuites judiciaires ou encore, entrait dans une phase de restructuration.

C'est pourquoi nous avons envisagé un objectif théorique de 15 entretiens tout en sachant que ce nombre était susceptible de varier au cours de la recherche. Nous devions, pour respecter le critère de saturation, observer au fur et à mesure des entretiens, le moment où les données récoltées n'apporteraient aucune information supplémentaire susceptible d'être utile à la recherche (Morse 1994; Pires 1997). Après le treizième entretien, nous avons constaté que l'information devenait quelque peu redondante mais parce que les cheminements de carrière des deux derniers participants étaient particuliers, nous pensions qu'ils auraient peut-être une façon différente d'appréhender la gestion du risque informationnel. La cueillette d'information s'est donc achevée au bout de quinze entretiens d'une durée variant entre 60 et 90 minutes chacun.

3.2.1 Caractéristiques de l'échantillon

Les participants rencontrés proviennent de petites, moyennes ou grandes entreprises. Ces entreprises œuvrant pour la plupart dans la production et la distribution de biens et de services sont issues d'industries aussi diverses que le transport, les télécommunications, le commerce de détail, la sécurité ou les ressources naturelles. De façon générale, ils poursuivent le même objectif mais les moyens humains et financiers pour les atteindre ne sont pas de la même envergure. Pour les raisons mentionnées précédemment, nous n'avons été en mesure de rencontrer que quatre gestionnaires de la sécurité/sécurité de l'information provenant de PME.

Le tableau de l'annexe A dresse un portrait des entreprises pour lesquelles œuvrent les gestionnaires de la sécurité/sécurité de l'information. En résumé, les répondants proviennent majoritairement de grandes entreprises (onze répondants sur quinze), l'un provient d'une moyenne entreprise et les trois autres d'entreprises de petites envergures.[15]Ces entreprises évoluent dans différentes industries (transport, médias, sécurité, logiciels, ressources naturelles et commerce de détails). Même si six de nos répondants proviennent du commerce de détails, leurs particularités respectives n'enlèvent rien à la richesse des données. Aussi, comme nous devions respecter certains critères liés à la diversification interne de l'échantillon, nous avons choisi de nous entretenir avec des gestionnaires de la sécurité issus du milieu policier (ou militaire) et du milieu civil. Les domaines d'expertise ont aussi été considérés lors de la constitution de l'échantillon; la protection du patrimoine informationnel n'étant pas l'apanage exclusif des informaticiens ou des gestionnaires de risques (*risks managers*). Au total, 15 individus ont été rencontrés. Les participants sont tous des hommes âgés entre 35 et 60 ans. Trois d'entres eux sont des policiers ou militaires à la retraite alors qu'un seul, auparavant policier-militaire, a choisi de réorienter sa carrière vers l'entreprise privée. Ces derniers occupent tous des fonctions liées à la protection des actifs physiques au sein

[15] Structure selon le nombre d'effectifs. Petites entreprises : moins de 100 employés. Moyennes entreprises : entre 100 et 499 employés. Grandes entreprises : plus de 500 employés. Source : *Industrie Canada*. http://www.ic.gc.ca/eic/site/061.nsf/fra/02719.html

de grandes entreprises tandis que les gestionnaires de la sécurité de l'information ou gestionnaires TI sont issus du milieu civil et se répartissent entre les petites et les grandes entreprises. Il est également pertinent de noter que les anciens militaires gèrent la sécurité dans des organisations dont les risques globaux sont considérés comme élevés.

3.2.2 Profils des répondants

La majorité des participants évolue dans le domaine de la sécurité depuis qu'ils ont quitté les bancs d'école. C'est d'ailleurs le cas pour tous les gestionnaires en sécurité. Pour ce qui est des gestionnaires T/I, l'aspect sécuritaire s'est greffé progressivement au poste pour devenir une fonction en soi. Pour deux d'entres eux, la sécurité de l'information, quoique déjà présente par l'entremise de certains mécanismes, s'est vue accentuée par des obligations contractuelles liées aux activités de l'entreprise. Quant à la formation académique des participants, celle-ci est fort variée au sein de l'échantillon. La plupart des participants ont minimalement une formation collégiale couplée d'une formation spécialisée provenant d'un corps policier ou militaire pour quatre d'entre eux.

Quant aux gestionnaires TI, cinq répondants sur six ont une formation universitaire et fait qui n'est peut-être pas étonnant, ce sont les mêmes cinq répondants qui sont membres d'un comité de gouvernance ou membre du conseil de direction (voir le tableau de l'annexe B). Faire partie d'un réseau professionnel semble être une particularité partagée par la majorité des répondants mais nous y reviendrons amplement dans le chapitre consacré à l'analyse.

3.3 Cueillette de données

La cueillette de données, communément appelée le «terrain», s'est déroulé durant les mois de janvier à octobre 2012. Nous mentionnerons plus loin les raisons qui nous ont poussées à étendre la recherche de participants sur une période aussi longue. Il faut savoir que huit entretiens se sont déroulés entre les mois de février et avril, deux furent réalisés au mois de juin, un au mois de septembre et cinq au mois d'octobre.

Afin d'engager la communication avec un nombre suffisant d'entreprises, les contacts personnels et professionnels se sont avérés indispensables. Pour la moitié d'entres eux, la prise de contact initiale s'est effectuée par téléphone et ensuite, une courte description du projet a été transmise par courriel. Quant à la seconde moitié des participants, la communication s'est effectuée essentiellement par courriel. Le projet a aussi été transmis aux membres de l'organisation ASIS, chapitre de Montréal. Un seul individu a répondu à l'appel. Étant donné la sensibilité du sujet (comme nous l'avons expliqué plus tôt), être confronté à un taux particulièrement élevé de refus et d'absence de réponse est une problématique à laquelle nous nous attendions : c'est d'ailleurs pourquoi la collecte de données s'est étendue sur une aussi longue période. Ainsi, une fois le premier contact établi, nous avons entrepris de fixer des rendez-vous avec les personnes intéressées.

3.3.1 Condition de réalisation des entretiens

En ce qui concerne les conditions de réalisation des entretiens, le choix du lieu et de la date a principalement été déterminé selon les disponibilités du participant. Nous avons cependant suggéré que l'entretien ne se déroule pas dans le bureau du gestionnaire mais plutôt, dans un autre local à l'intérieur de l'entreprise et ceci, pour deux raisons : éviter d'être interrompu durant l'entretien (nous en rediscuterons plus loin) et conserver la dimension contextuelle de l'entreprise. Sur les 15 participants rencontrés, cinq d'entres eux ont utilisés leur bureau alors que neuf autres ont privilégiés la salle de conférence.

Un seul participant a choisi de me rencontrer dans un café attenant les bureaux administratifs de la société. Ce choix pourrait s'expliquer par la nature des activités de l'entreprise, activités qui impliquent un risque d'espionnage potentiellement élevé, comme en témoigne son historique.

Les trois premiers entretiens ont débuté avec une consigne initiale qui s'articulait de la façon suivante : «Comment s'effectue la gestion des risques informationnels dans votre entreprise?» Après retranscription des discours, on pouvait rapidement se rendre compte qu'après quelques minutes, il fallait revenir au point de départ afin de mieux définir l'objet de l'entretien. C'est pourquoi il a été nécessaire de reconsidérer la consigne initiale en intégrant une définition du risque informationnel qui demeurait somme toute, relativement large. Cette consigne a pris la forme suivante : «Comment s'effectue la gestion des risques informationnels dans votre entreprise ? Par risques informationnels, j'entends par là, tout ce qui peut menacer l'intégrité des données confidentielles de votre entreprise?» Présentée de cette façon, la consigne «…définit le thème sur lequel l'interviewé est invité à s'exprimer» tout en favorisant l'expression des «schémas mentaux» propre à chaque individu (Fenneteau 2002, p.20-21).

Au cours de l'entretien, nous devions, pour atteindre les objectifs de notre recherche, discuter intégralement de quatre grands thèmes. Chaque thème, en lien direct avec les objectifs spécifiques de la recherche, comportait plusieurs sous thèmes, lesquels ont été évoqués spontanément par plus de la moitié des participants. Les quatre principaux thèmes devant être abordés étaient les suivants :

1) le patrimoine informationnel;
2) le processus d'identification et de hiérarchisation des risques (ou menaces);
3) la dynamique entre les intervenants (internes et externes);
4) le rôle et les responsabilités du gestionnaire de la sécurité en matière de gestion des risques informationnels.

Dans la plupart des cas, la prise de notes s'est avérée un instrument efficace de rappel puisque certains discours étaient relativement décousus et d'autres, plutôt passionnés. La dynamique propre aux relances en fut ainsi simplifiée.

3.3.2 Cadre contractuel de l'entretien

Avant que les entretiens ne débutent, certaines règles de conduites devaient être respectées. En premier lieu, je devais me présenter et définir les rôles de chacun en créant, dans la mesure du possible, un climat de confiance et de crédibilité. Ensuite, je devais revenir brièvement sur les «finalités» de l'étude en m'assurant que le participant saisi bien l'importance de l'entretien qui allait se dérouler (Poupart 1997). «Cela souligne l'utilité du travail que l'interviewé va effectuer et l'encourage à parler» (Fenneteau 2002, p.18). Le document intitulé «Renseignements aux participants» a servi de cadre à cet exercice. Une fois ces points clarifiés, le formulaire de consentement a été remis au participant. Notons que plus de la moitié d'entres eux ont préféré recevoir une copie de ce formulaire par courriel avant la tenue de la rencontre. Il a aussi été utile de répéter au participant que l'information transmise serait traitée selon des règles très strictes de confidentialité et d'éthique imposées par l'université. Chaque participant a aussi été avisé qu'il était libre d'accepter ou de refuser d'être enregistré : un seul participant a refusé d'être enregistré. Avant chaque entretien, il fallait souligner l'importance d'utiliser un magnétophone dans la mesure où l'intégralité du discours permet de demeurer fidèle aux propos du participant. La durée de l'entretien a aussi été précisée en insistant sur le fait qu'il est essentiel de ne pas être interrompu en cours de route. En plus de prolonger l'entretien, ces interruptions involontaires peuvent affecter la fluidité du discours et donc interférer sur les schémas cognitifs du participant.

Finalement, afin de pouvoir procéder à une analyse rigoureuse, il a été nécessaire de créer deux fiches signalétiques : l'une pour l'entreprise, l'autre pour le gestionnaire. Ces deux fiches, qui peuvent être consultées en annexe, ont pu être complétées avant la tenue de l'entretien. Le fait d'avoir pris connaissance de ces documents (fiches signalétiques et

formulaire de consentement) avant la rencontre m'a permis de respecter le temps (1h30) qui m'était alloué et par le fait même, a facilité le bon déroulement de l'entretien.

3.4 Stratégie analytique

Une retranscription intégrale de chaque enregistrement audio a été effectuée durant les heures suivant l'entretien. En étant encore imprégné de l'expérience, il s'avère plus facile de commenter certains passages qui nous auraient laissé une impression particulière non perceptible à travers le document audio comme le langage non verbal ou le contexte interactionnel. Une fois retranscrit, chaque entretien a ensuite été analysé manuellement et ceci pour deux raisons : certains entretiens se sont déroulés tant en anglais qu'en français alors que deux des participants ont souhaité de pas être enregistré. Ces entretiens ont dû être entièrement manuscrits. C'est à partir d'une analyse thématique que nous avons pu «procéder systématiquement au repérage, au regroupement et subsidiairement, à l'examen discursif des thèmes abordés» (Paillé et Mucchielli 2005 p.124). L'analyse thématique a donc été constituée de plusieurs étapes. À l'intérieur de chaque étape, nous avons privilégié une démarche itérative et incrémentale; "itérative" dans le sens où la démarche se décompose en étapes successives par lesquelles on passe incessamment, "incrémentale" pour signifier que la base de connaissances s'enrichit de nouvelles informations à chaque tour (Culet 1994). Après une analyse verticale de chaque entretien, une analyse transversale a été effectuée, c'est-à-dire que nous avons procédé à une comparaison des entretiens à partir des thèmes, catégories et concepts importants qui ont été préalablement identifiés (Paillé et Mucchielli 2005). Ces données qui pourront être consultées à l'annexe C reprend les thèmes, catégories et sous-catégories ayant émergés de cette analyse.

3.5 Limites

Nous devons finalement aborder la question des limites. D'abord, il est essentiel de se rappeler que peu importe la méthodologie préconisée, le chercheur fera toujours face à un certain nombre de limites. La subjectivité relative à l'interprétation des données constitue la première de ces limites; non pas parce que nous parlons de méthodes qualitatives mais plutôt parce que nous devons être conscient que la complexité de la réalité sociale est difficilement objectivable. Qui plus est, nul ne peut prétendre que la relation entre le chercheur et son sujet ou entre le chercheur et ses données, relève d'un processus neutre. Selon Quivy et Van Campenhoudt : «Les propos de l'interviewé sont toujours liés à la relation spécifique qui le lie au chercheur et ce dernier ne peut donc les interpréter valablement que s'il les considère comme tels» (p.187). En tenant compte du principe de réflexivité, il est donc possible de surmonter cette limite. Dans le contexte particulier de cette recherche, il faut aussi prendre en compte que l'introduction d'une étude sur des pratiques de gestion des risques peut déjà influencer la perception du sujet quant à ce risque et donc, introduire un «biais» dans l'interprétation des résultats. De plus, le gestionnaire aura peut-être tendance à dissimuler ce qu'il ne fait pas et à dévoiler avec grand intérêt ce qui est accomplit par lui-même ou par son entreprise. Là encore, il s'agira d'être prudent, autant lors des entretiens que lors de l'interprétation des résultats.

Finalement, lorsque nous abordons la sécurité de l'information, la sensibilité du sujet demeure l'une des limites les plus importantes du point de vue de la collecte de données. La plupart des refus relevaient d'ailleurs de l'impossibilité pour le gestionnaire de discuter de cette dimension de son travail et cela, même en tenant compte de l'aspect confidentiel et anonyme de la recherche. Le faible taux de participation est aussi dû au temps qu'un gestionnaire peut consacrer à un projet universitaire. Toutefois, nous avons pu constater qu'une fois le dialogue amorcé, le gestionnaire comprend rapidement qu'il s'agit d'un engagement à très court terme et qu'un entretien peut très bien se boucler en moins d'une heure lorsque l'objectif est clair et que l'intervieweur est bien préparé.

Quoi qu'il en soit, il sera toujours possible de nuancer les effets des différentes limites associées à l'utilisation de la méthodologie qualitative. Comme Miles le souligne: «(…) the nuisances can be reduced by thoughtful methodological inquiry» (Miles 1979, p. 590). À cela, nous ajouterons que la rigueur, la justesse et l'adaptabilité des résultats (à ne pas confondre avec généralisation) sont autant de critères qui rendront le travail de recherche crédible et scientifiquement valable (Laperrière 1997).

CHAPITRE 4. ANALYSE DES DONNÉES

4. Analyse des données

Quelle que soit la taille de l'entreprise, les enjeux liés à la protection de l'information ne sont définitivement plus les mêmes qu'il y a quelques années. L'évolution de la technologie numérique et l'utilisation effrénée des appareils mobiles complexifient la protection des actifs et transforment les risques liés à la sécurité de l'information. Non seulement les risques se multiplient, mais leur gestion nécessite la collaboration de plusieurs acteurs stratégiques qui gravitent autour d'un ou de plusieurs individus responsables de la sécurité au sein de l'entreprise. La plupart de ces individus, qui n'occupent pas nécessairement une fonction dédiée entièrement à la sécurité de l'information, n'en sont pas moins responsables à divers degrés. Comme nous l'avons souligné à maintes reprises dans les chapitres précédents, le rôle du gestionnaire de la sécurité ne se limite plus à la protection physique des biens et des personnes : il doit maintenant veiller à protéger tant le patrimoine matériel qu'immatériel de l'organisation en s'assurant d'avoir les compétences et connaissances adéquates pour accomplir une telle tâche ou en s'alliant à des experts capables de le faire.

Dans un tel contexte, il devient impératif de traiter la gestion des risques informationnels comme un enjeu global qui implique des gestionnaires issus de différentes professions et qui occupent des fonctions aussi variées que les domaines d'activités des entreprises qui les emploient. Ce chapitre ne vise donc pas à effectuer une comparaison entre les gestionnaires TI et les gestionnaires de la sécurité : il vise plutôt à comprendre comment s'effectue la gestion des risques informationnels dans l'entreprise privée et quelles sont les forces qui entrent en jeu lors du processus décisionnel. Conséquemment, nous aborderons la gestion des risques informationnels selon la perspective du gestionnaire qui en a la responsabilité, peu importe le titre qu'on lui a octroyé; qu'il soit directeur de la sûreté, directeur de la sécurité globale, directeur des systèmes d'information ou responsable des technologies de l'information.

Dans le présent chapitre, nous traiterons, dans un premier temps, de la gestion des risques informationnels à travers trois principales dimensions: l'aspect contextuel, l'aspect relationnel et le profil du gestionnaire de la sécurité. L'analyse de ces dimensions nous permettra d'identifier les principaux éléments qui viennent influencer le processus décisionnel de gestion des risques informationnels. Comme il est question d'une structure dynamique où chaque élément peut exercer un effet sur un autre élément du modèle, il est nécessaire de les traiter séparément et cela, afin de préserver la clarté du texte et de favoriser la compréhension de l'analyse.

La deuxième partie de ce chapitre sera consacrée à la dynamique structurelle qui permet de lier ces éléments, de leur conférer une certaine cohérence. C'est dans cette partie que nous conclurons l'analyse en tenant compte des prémisses de bases de l'approche multidimensionnelle du risque et de l'approche de la transaction sociale. Cette analyse nous permettra de mieux appréhender la gestion des risques informationnels dans une entreprise privée. Nous pourrons ainsi répondre aux objectifs spécifiques de ce mémoire qui consistent à comprendre comment s'effectue le processus d'identification et de hiérarchisation des risques lorsqu'il est question de la protection du patrimoine informationnel. Nous serons aussi en mesure de connaître les dynamiques qui existent entre les acteurs internes et externes qui interviennent dans ce processus. Et finalement, nous pourrons saisir le rôle du responsable de la sécurité en matière de gestion des risques informationnels et ce, à chaque étape du processus : de l'identification du risque à la mise en application des mesures de sécurité.

4.1 L'ASPECT CONTEXTUEL

4.1.1 De quel type d'enjeux est-il question?

Pour être en mesure de comprendre comment s'effectue la gestion des risques informationnels, il faut d'abord savoir que le secteur d'activités de l'entreprise, le

contexte (règlementaire, économique, politique) dans lequel elle évolue et son degré d'influence sur différentes sphères de la société (environnement, économie, politique) déterminent, en quelque sorte, les enjeux auxquels les gestionnaires auront à faire face. Pour citer l'un des interviewés rencontrés : «Y a des entreprises qui ont beaucoup plus d'enjeux que nous autres» (Interviewé 5). Dans cette section, nous ferons cependant fit des éléments contextuels généraux, qui exercent une influence relativement comparable sur tous les départements d'une entreprise comme les cycles économiques, les changements politiques et certaines lois ou règlements.[16]

Par exemple, dans le commerce de détails, ce sont les transactions POS (Point Of Sale)[17] et le vol de données liées aux cartes de crédits qui constitue l'enjeu le plus important au niveau du risque informationnel. Pour d'autres, l'enjeu se situe à l'interne et se traduit par le comportement malveillant des employés. En parlant de la fraude, l'interviewé 11 déclare que: «Personnellement qu'est-ce que je pense, c'est plus de 85% est faite à l'interne pis la balance a vient de l'externe». Cependant, lorsqu'il est question d'une entreprise qui compte près de 100 000 travailleurs répartis à travers le monde, la fraude, à petite échelle, n'est pas ce qui préoccupe le plus le gestionnaire de la sécurité. Les enjeux sont multiples et l'impact d'une mauvaise gestion des risques informationnels peut avoir des conséquences désastreuses qui vont au-delà de la survie de l'entreprise et qui pourraient se répercuter sur l'économie ou la politique d'un pays. Pour ce type d'entreprises, il est par exemple question d'enjeux liés aux activités d'espionnage industriel et aux prises de contrôle hostiles.

> «Ce qui est arrivé, c'est qu'on a eu des tentatives hostiles de take over. Il a fallu se battre contre ça…y a des gros deals qui ont fouerrés à cause de fuites, d'exfiltration. Ils ont été attaqués, ils ont vu ce qui se passait. Ce qu'il faut comprendre c'est que ces deals-là se font en cachette à cause des actions, des délits d'initiés…on est là-dedans» (Interviewé 8).

[16] La décision de ne pas les aborder est basée sur la nécessité de synthétiser la matière la plus pertinente.
[17] Point de vente où le paiement peut s'effectuer avec carte à partir d'un terminal.

Au Québec, certaines sociétés «se sont dotées d'une structure de capital qui les mettent à l'abri de tentatives de prise de contrôle» (Allaire 2012, p.3) par exemple, en étant la propriété d'un ou de quelques actionnaires reliés. Trois des 15 gestionnaires de la sécurité que nous avons rencontrés font partie de ces sociétés et c'est la raison pour laquelle ils ne sont pas inquiets outre mesure par des prises de contrôle hostiles provenant de la concurrence.

Par ailleurs, plus des deux tiers des interviewés ont répondu que préserver la réputation de l'entreprise demeure un enjeu majeur auquel ils ne peuvent se soustraire. «Il y a des dossiers qui pourraient être hautement médiatisés, des personnes de tout niveau, que ce soit politique, financier, que ce soit réputation, on touche à peu près à tout. C'est une chose excessivement sensible» (Interviewé 10). L'interviewé 3 tient des propos similaires lorsqu'il fait référence aux médias et à l'impact qu'une mauvaise presse pourrait avoir sur l'entreprise : «Est-ce qu'on est préoccupé de faire la une du journal de Montréal parce qu'on a eu un bris de sécurité, oui tout à fait! Sans dire que ça guide…ça nous tient sérieux dans la démarche».

Durant les entretiens, trois des quinze gestionnaires interviewés ont fait mention d'un autre enjeu qui, selon eux, constitue la prémisse de base de la gestion des risques informationnels, soit la capacité à identifier ce qui constitue l'information sensible, confidentielle ou secrète de l'entreprise. Comme le souligne l'interviewé 8 :

> «Tu ne peux pas dire à des gens "Tu m'as volé du secret, tu m'as volé du brevet ou de la propriété intellectuelle !" si tu ne la protèges pas ou si les gens ne savent pas que ce que tu leur confies est de la propriété intellectuelle et qu'ils n'ont pas signé une entente de confidentialité».

Dans un même ordre d'idée, le savoir-faire de l'entreprise est un point qui a aussi été soulevé à quelques reprises par certains interviewés. Bien que les gestionnaires de la sécurité soient conscients que le savoir-faire fasse partie intégrante du patrimoine informationnel de l'entreprise, il est encore ardu d'en définir adéquatement les critères.

«(…) Le comment, le pourquoi, les façons de faire, le type de sécurité, c'est considéré comme très important et très vital à l'entreprise» (Interviewé 10). Les propos de l'interviewé 8 vont dans le même sens lorsqu'il affirme que ce n'est que récemment que l'entreprise s'est aperçu que leur savoir faire, ce qu'ils appellent «leurs processus», représentait un actif de propriété intellectuelle et que de fait, il fallait la protéger. Si l'on considère que certains types d'appropriation malveillante d'information et d'expertise existaient bien avant la naissance de l'informatique, cette prise de conscience relativement nouvelle (Santoni 2006; CIGREF 2007; Denis 2009) est surprenante, surtout lorsqu'on la constate dans de grandes entreprises positionnées sur le marché mondial.

Quant à l'information financière, la plupart des participants nous ont mentionnés qu'il ne s'agit pas d'une préoccupation majeure en termes de risques informationnels. À ce sujet, deux raisons bien différentes ont été invoquées : l'entreprise est publique et par conséquent, les résultats financiers sont accessibles. La deuxième raison étant que l'entreprise n'est pas suffisamment importante pour attirer la convoitise d'un concurrent. Du moins, c'est ce que rapportent deux des trois interviewés (S7 et S9) à qui nous avons posé la question. Faut-il en déduire qu'une entreprise qui n'est pas cotée en bourse est moins intéressante d'un point de vue concurrentiel? Non pas que les gestionnaires de la sécurité en sont convaincus mais leur patron, propriétaires desdites entreprises, semblent le croire.

Finalement, on ne pourrait passer sous silence ce qui, aux yeux des gestionnaires de la sécurité, représente l'un des plus grands défis sécuritaires que les entreprises doivent relever actuellement : les nouvelles technologies. L'utilisation des appareils intelligents et la gestion en nuage (cloud) sont, semblent-ils, deux éléments particulièrement ardus à gérer et à contrôler. L'interviewé 5 nous fait part de ses craintes à ce sujet :

> «(…) y vont se servir du cloud pour entreposer l'information à quelque part…oui mais c'est pas sous ton contrôle faque si c'est pas sous ton contrôle, tu sais pas c'est qui qui peut avoir accès à cette information-là. Des

> fois, c'est de l'information confidentielle, stratégique d'entreprise, surtout quand on parle d'un conseil d'administration faque là, ça me fatigue. On perd le contrôle! Et ça, c'est un risque majeur».

La plupart des interviewés nous répondent que les décisions d'affaires doivent se prendre en fonction des risques mais aussi en fonction de la fonctionnalité des appareils et des besoins de l'entreprise. Tous s'entendent sur la nécessité d'établir des procédures et politiques d'utilisation adéquates avant d'acquérir une nouvelle technologie. «On ne peut pas plonger dans une stratégie d'ouverture au niveau des téléphones intelligents par exemple, sans avoir backer tes arrières» (Interviewé 12). Les propos de l'interviewé 14 soutiennent cette affirmation : «Présentement, l'entreprise ne supporte ou n'acquiert pas d'appareils intelligents 'at large' car il n'y a aucune politique de contrôle». Les gestionnaires de la sécurité ont aussi abordé la problématique de l'espionnage industriel et du piratage informatique de même qu'ils nous ont fait part de l'anonymat que confèrent les nouvelles technologies, de son caractère transnational et de la vitesse à laquelle les données pourraient s'envoler. Selon eux «plus la technologie avance, plus le risque grandit» (Interviewé 10). «Aujourd'hui, tu peux pu vivre sans les TI et tes vulnérabilités viennent des TI» (Interviewé 5).

La situation est doublement problématique puisque la demande de nouvelles technologies provient des clients mais aussi des employés qui souhaitent améliorer leur efficacité au travail. «(…) Mais de dire où on va être dans six mois… mais comme je dis, on ne peut pas dire non au progrès, on ne peut pas dire non au client» (Interviewé 10). Et cela, est sans compter les membres de la direction, qui, selon les interviewés, n'attendent pas la mise en place de politiques de sécurité pour utiliser leur appareil intelligent à des fins professionnelles, exposant du même coup les données stratégiques de l'entreprise à des esprits futés et malveillants. «Le IPad c'est très sexy mais pour voyager, c'est très difficile de mettre des politiques de sécurité dessus» (Interviewé 8).

Néanmoins et malgré le risque, il n'est plus question de choix, selon une majorité des gestionnaires interviewés. «Le train s'en vient là tsé, à grande vitesse puis il faut se positionner tout de suite. On n'a pas le choix pis on pourra pas dire non» (Interviewé 5). Le constat est le même pour l'interviewé 10 qui déclare : «On est un peu esclave de la technologie. La demande vient vite, l'exigence de la réponse est rapide et les outils que tu utilises pour faire ça sont aussi très rapides mais sont très vulnérables».

Adopter de nouvelles technologies implique également des contraintes légales et opérationnelles notamment avec la tendance BYOD (Bring your own device)[18]. Non seulement l'infrastructure des systèmes d'information doit être adaptée à l'utilisation d'appareils personnels mais des politiques de sécurité doivent être conçues spécifiquement à cet effet. Les propos de l'interviewé 8 résument bien la situation qui prévaut dans les entreprises :

> «Le problème qu'on a parfois c'est qu'on doit faire des interventions pour voir ce qui se passe et on est pris avec des contraintes légales (…) si tu dis à la personne, amènes ton propre «device», et que tu lui installes peu importe la solution (…) et qu'il arrive quelque chose et que tu «wipes»[19] la machine, ça va pas bien parce que la personne peut dire où sont mes photos, où sont mes affaires personnelles?»

Les gestionnaires de la sécurité se retrouvent donc face à une situation où l'utilisation des nouvelles technologies et les risques qu'elles comportent s'équilibrent difficilement. Les sondages que nous avons consultés[20] tendent à confirmer cette prémisse. Les innovations propres aux technologies de l'information se multiplient à une vitesse telle que les gestionnaires de la sécurité peinent à suivre le rythme et à adapter leur politique en conséquence. Cet aspect du contexte organisationnel semble être pour les gestionnaires de la sécurité, l'un des enjeux les plus difficilement contrôlables. Non

[18] Les employés apportent leur appareil personnel pour travailler (ordinateur portable, tablette, téléphone intelligent)
[19] Procédure qui consiste à supprimer définitivement les dossiers et fichiers d'un appareil.
[20] PWC, Ernst & Young, Deloitte, Verizon.

seulement doivent-ils composer avec des variables technologiques de plus en plus complexes mais ils doivent aussi transiger, en parallèle, avec des variables humaines, financières et légales qui imposent, exigent et tentent de négocier une utilisation plus ou moins rigide, selon le cas, des outils technologiques mis à leur disposition. Cette délicate imbrication des interactions sociales et de la gestion des enjeux propres au contexte de chaque organisation démontre l'utilité de notre approche puisque la dynamique relationnelle semble se révéler indissociable de l'analyse multidimensionnelle des risques informationnels.

4.1.2 Contraintes et opportunités

Comme nous l'avons constaté, le contexte, c'est aussi un nombre incalculable de contraintes et d'opportunités qui se présentent à l'entreprise et au gestionnaire de la sécurité. À ce sujet, la majorité des interviewés ont perçu, dans un même élément, autant de contraintes que d'opportunités. Par exemple, l'interviewé 12 mentionne que «le fait de devoir rencontrer des normes et standards nationaux apporte certaines contraintes mais en même temps, cela force les entreprises à augmenter leurs propres standards à l'interne». Pour ce gestionnaire, la contrainte permet de s'améliorer, de se dépasser. Lorsque nous avons demandé à un gestionnaire de la sécurité informatique si les lois et règlements représentaient des contraintes importantes, celui-ci nous a répondu : «J'trouve pas. Y faut s'adapter tout simplement. Les lois, on n'a pas le choix, faut les respecter» (Interviewé 5).

D'autres n'y voit cependant que des contraintes. En fait, un seul interviewé s'est exprimé de la sorte : «Dans le cas des cartes de crédit, je dirais que c'est juste des contraintes. Je vois pas quel avantage on aurait à appliquer ces normes-là[21]. C'est pas nous qui est à risque dans le fond, c'est nos clients, c'est les banques qui sont à risque» (Interviewé 14). Dans le secteur de la vente au détail, tous les gestionnaires interviewés nous ont parlé des normes PCI DSS. Ces normes ont été élaborées par le *Conseil des normes de*

[21] Normes en matière de sécurité des données PCI DSS (Payment Card Industry Data Security Standards)

sécurité du secteur des cartes de paiement et visent à «améliorer la sécurité des données de comptes de paiements»[22]. Fondé par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc., ils en partagent la gouvernance et exigent de leurs utilisateurs (les commerçants) qu'ils respectent les normes établies.

Par ailleurs, au sein de quelques-unes des entreprises de notre échantillon, il est nécessaire, pour répondre aux exigences de contrats gouvernementaux particuliers, d'obtenir une cote de sécurité de niveau «secret» ou «très secret». L'interviewé 10 nous explique quelles mesures ont été appliquées afin qu'un département réponde à ces exigences : «(…) on a dû faire une ségrégation totale de son groupe (…) parce qu'elle est informatisée quasiment à 100%. Le niveau de sécurité informatique est très élevé, y a un groupe qui prend soin juste de son département». Un autre gestionnaire nous a fait part des modifications qu'il devra apporter pour améliorer l'ensemble des mécanismes de sécurité en place (de la gestion des accès à l'architecture de son système informatique) afin de pouvoir réaliser les conditions de son contrat avec le gouvernement (Interviewé 7). Dans ces deux cas particuliers, il est question de contraintes similaires qui touchent d'un côté, une entreprise de moins de quarante employés et de l'autre, une entreprise qui en compte des milliers.

La différence se situe peut-être davantage au niveau de la lourdeur du processus décisionnel des grandes entreprises qui semble être une contrainte récurrente à la gestion des risques informationnels. Il implique davantage d'individus et est largement plus fastidieux dans son application, ne serait-ce que dans la transmission des procédures, des règles de sécurité, et de la mise en place des mesures de contrôle. Selon l'interviewé 10, «les mesures doivent être instaurées dès le processus de sélection des candidats». Au moins cinq autres interviewés ont soulevé ce point, mentionnant entre autres, qu'une enquête pré-emploi (situation financière et antécédents judiciaires) est requise auprès de tous les nouveaux employés. Pour parer cette contrainte organisationnelle, certains interviewés ont aussi discutés de la mise en place de rapports hebdomadaires ou journaliers afin d'être en mesure d'établir des statistiques et d'être au fait des

[22] https://frca.pcisecuritystandards.org/minisite/en/index.php

incohérences et des accès non autorisés dans les systèmes. Dans les plus petites entreprises, cette contrainte est quasi-inexistante puisqu'il est possible, pour un gestionnaire, de rencontrer personnellement tous les employés afin de les informer des politiques de sécurité et des procédures à suivre en termes de protection de l'information.

Finalement, la seule contrainte n'ayant pas trouvé son pendant positif, est la contrainte budgétaire. Bien que plus de la moitié des interviewés nous ont mentionné avoir peu de difficulté à obtenir du financement pour certains projets à moyen ou long terme, la sécurité est encore l'un des secteurs qui écope le plus lorsqu'il y a compressions budgétaires. «(…) l'exemple que je donnais tantôt c'est on a le choix de prioriser un dossier opération de magasin ou un dossier de sécurité ben on sait c'est quoi» (Interviewé 5). Pour la jeune entreprise, deux discours s'affrontent : les mesures de sécurité doivent être mises en place dès le départ ou le temps et l'argent doivent être utilisés à d'autres fins, comme la recherche et le développement, la publicité, la mise en marché, l'embauche de personnel, etc. À ce sujet, l'interviewé 3 nous fait part de sa position quand aux contraintes associées au budget dédié à la sécurité :

> «En fait, on est une nouvelle organisation qui est en phase de démarrage. À date, on a toujours agit en personne raisonnable pour voir qu'est-ce qui est requis «custom doing business». J'dirais que les premières années, faut faire ce qu'il y a à faire pour que ça soit bien fait».

Pour certains interviewés, la contrainte se situe davantage au niveau de l'attitude réfractaire des dirigeants par rapport à ce que la sécurité apporte concrètement à l'entreprise, le «retour sur investissement» étant encore difficile, voire impossible à chiffrer de façon réaliste et convaincante. Nous pouvons également retenir que lorsque nous parlons de contraintes ou d'opportunités, nous faisons référence à des concepts relativement subjectifs qui puisent leur signification à travers l'expérience et la personnalité de chaque gestionnaire. Si certains arrivent à retirer des avantages d'une situation contraignante, d'autres ni verront que des inconvénients. D'un point de vue comme de l'autre, cette attitude influencera le processus décisionnel dans lequel le

gestionnaire s'engagera lorsqu'il sera question de gestion des risques informationnels. Encore une fois, nous soulignons l'importance de considérer les interactions comme des jeux de pouvoirs et de contre-pouvoirs où les contraintes deviennent l'objet de négociations, de conflits au sein d'un processus décisionnel qui vise un objectif somme toute, commun, la réduction des risques informationnels.

4.1.3 La tolérance au risque

Finalement, un dernier point doit être abordé puisque son influence sur le processus décisionnel du gestionnaire de la sécurité est significative: la tolérance au risque. La tolérance au risque, rappelons-le, est le «degré de risque qu'une organisation est capable d'accepter» (Ebondo Wa Mandzila & Zéghal 2009, p. 19). Par définition, elle est relative et dépend de plusieurs facteurs, notamment, du style de gestion privilégié par les dirigeants. «(…) J'veux dire, c'est ça la sécurité, c'est toujours (…) c'est la balance entre le prix que ça te coûte et c'est quel niveau de sécurité que tu veux avoir, quel prix t'es prêt à mettre versus qu'est-ce que t'es capable de vivre avec» (Interviewé 11).

D'autres sont plus prudents comme en fait foi les propos de l'interviewé 12 : «On n'est pas une très grande entreprise internationale alors nos succès dépendent aussi de la prudence qu'on a eu face à certaines décisions». En fait, ce que nous constatons, c'est que la tolérance au risque n'est pas relative à la taille de l'entreprise mais correspond plutôt à son stade de développement et à la personnalité des dirigeants. Par ailleurs, comme deux des quinze interviewés (9 et 10) offrent aussi de la sécurité à l'externe, non seulement ils sont contraint de tenir compte de la tolérance au risque des membres de la direction de leur entreprise mais ils doivent aussi travailler avec la tolérance aux risques de leurs clients. Voici ce que l'interviewé 10 avait à dire à ce sujet :

> «(…) entre les deux c'est quoi mon choix? À titre d'exemple, nous on se donne des critères assez élevés à propos des informations de nos clients et le

client nous dit ‘non non non je veux pas l’avoir : c’est trop compliqué quand tu nous fais un code pour le e-mail’. Là, le client vient de faire son choix!»

Nous constatons ici que la mise en place de procédures et politiques relativement à la sécurité de l’information n’est pas uniquement tributaire du gestionnaire de la sécurité. Parce que la gestion des risques informationnels relève d’un processus dynamique, l’interaction de l’entreprise avec son environnement conduit le gestionnaire à modifier sa position, à s’adapter en fonction des enjeux, des contraintes et des opportunités qui se présentent à lui. Le degré de tolérance au risque varie également en fonction de nombreux facteurs puisqu’il dépend, en partie, des individus qui détiennent le pouvoir décisionnel. Les propos des gestionnaires nous amènent d’ailleurs à comprendre que ce pouvoir peut être parfois détenus par les clients et certains partenaires qui, ultimement, acceptent ou non de se plier aux exigences de sécurité de l’entreprise. Nous pouvons retenir que la gestion des risques informationnels implique non seulement de tenir compte d’un nombre important et changeant de facteurs contextuels mais il faut de plus, considérer l’ensemble des principes relationnels qui s’imbriquent au sein de ce processus.

4.2 L’ASPECT RELATIONNEL

4.2.1 Au sein de l’entreprise

Tel que nous l’avons écrit au chapitre 2, l’aspect relationnel pourrait se résumer à l’ensemble des interactions formelles et informelles qui interviennent dans le processus décisionnel du gestionnaire de la sécurité en matière de gestion des risques informationnels. À l’interne, ces interactions sont issues des rapports que le gestionnaire entretient avec la direction, les différentes divisions de l’entreprise le cas échéant, avec les autres départements ainsi qu’avec les employés dont il a la responsabilité.

Les questions relatives à la dynamique relationnelle à l'interne ont suscités en premier lieu, un vif intérêt pour le cas des vérificateurs. Huit entreprises de notre échantillon bénéficient d'un service d'audit interne. «(…) t'as besoin d'une structure pis la structure dans l'industrie habituellement ben ça passe justement par un genre de plan, de revue des problèmes et de l'analyse de la sécurité et ça, ça marche seulement si t'engage des auditeurs internes» (Interviewé 11). D'une part, ceux-ci s'impliquent activement dans certains projets comme le mentionne l'interviewé 5 : «Vérification interne vont aussi participer à différents projets stratégiques (…) vérification interne veut s'assurer que les bons contrôles vont être en place». D'autre part, ils sont perçus par certains comme des étrangers qui n'ont que très peu conscience de la réalité à laquelle les gestionnaires sont confrontés quotidiennement.

> «Souvent y disent 'ah y a rien là faire ça'. Y a tellement d'intervenants pour identifier les lacunes (…) t'as trois personnes qui ont accès à une base de données hautement confidentielle sauf que les auditeurs trouvent ça terrible quand même» (Interviewé 11).

En fait le travail des vérificateurs est de s'assurer «que la gestion des risques est efficace et que l'entreprise adhère aux bonnes pratiques en matière de gouvernance. Les travaux des auditeurs internes résultent en des recommandations visant à améliorer les processus, les politiques et les procédures»[23]. De manière générale, les propos de certains interviewés nous laissent croire que les auditeurs ou vérificateurs internes sont, en quelques sortes, un mal nécessaire, dont il faut s'accommoder. D'autres, sans toutefois les apprécier, les perçoivent davantage comme des partenaires qui contribuent à conserver la réputation de l'entreprise en matière de conformité[24].

Par ailleurs, l'interviewé 8, dont les responsabilités s'étendent au niveau mondial nous explique que les risques informationnels occupent une position centrale dans la matrice

[23] http://www.iai-quebec.ca/04_profession.htm.
[24] Notamment en vertu de la "Public Company Accounting Reform and Investor Protection Act"" et la "Corporate and Auditing Accountability and Responsibility Act". Adoptée par le sénat américain en 2002 et communément appelée Loi Sarbanes-Oxley. L'entreprise canadienne doit adhérer à ces normes si ces activités s'étendent au territoire américain.

des risques et que pour cette raison, «les exécutifs sont très au courant de ce qui se passe, (…) ils sont très très sensibilisés». De manière générale, les entreprises qui exploitent un marché national, nord-américain ou international se dotent de comité de gouvernance. Bien que les gestionnaires interviewés ne le désignent pas toujours ainsi, les fonctions et objectifs qui y sont rattachés sont relativement similaires d'une entreprise à une autre. Les propos de l'interviewé 14 résume en quoi peut consister un tel comité :

> «Il y a un comité de gouvernance des technologies de l'information. Le comité de gouvernance est composé d'officiers[25] du Québec (…) c'est un travail collectif. (…) Ce sont des choses dont on discute et qu'on adapte aux réalités. Il y a deux VP au Québec et il y a un représentant de chaque département. Ce comité a plusieurs responsabilités, entre autres, d'établir les politiques, de prioriser les projets. D'un point de vue informatique, je ne peux pas décider moi-même de faire un projet, il faut que ça vienne du comité de gouvernance. On peut proposer, mais on ne peut pas décider nous-mêmes de procéder sans avoir eu l'approbation de ce comité-là».

L'interviewé 6 emploie un vocabulaire similaire lorsqu'il parle de la façon dont s'organise la gestion des risques informationnels. Cependant, sa responsabilité, au niveau du groupe international, se limite davantage à une fonction d'exécutant :

> «Au bureau de Montréal, on applique la sécurité selon les besoins du bureau. L'équipe mondiale met en place des processus qui doivent être appliqués en plus de ce qui se fait déjà. La sécurité répond de la ligne d'affaires. Il y a instauration de processus et au bureau de Montréal, il y a application du processus, accompagnement et sensibilisation auprès des employés».

Dans une autre entreprise, le gestionnaire nous explique que chaque projet est amené sous la forme d'un «business case». Ce «business case» est ensuite soumis au vice-

[25] Anglicisme du terme «officer» qui peut se traduire par «cadre supérieur»

président qui lui, aura à décider s'il alloue les ressources. «C'est toujours le vice-président qui va avoir le portefeuille». Ce même gestionnaire ajoute que lorsqu'ils doivent instaurer de nouvelles procédures, «y va avoir un système qui est très complexe : affaires publiques, session de training, finances, département légal, IT security, à cause de l'image, de la réputation de la compagnie» (Interviewé 2).

L'interviewé 5 nous parle plus précisément d'un comité de sécurité qui se réunit trimestriellement. Le mode de fonctionnement ressemble aux cas précédents et les participants qui y siègent occupent des fonctions assez comparables : «(…) on va amener les risques élevés à ce comité-là et puis qui participent à ce comité, il y a la vice-présidente TI, le v.-p. r. h., services juridiques, vérification interne et moi».

L'un des gestionnaires interviewés nous a quant à lui mentionné qu'étant donné le nombre très élevé de risques de même que l'impact que la matérialisation de ces risques pourrait avoir sur l'entreprise, celle-ci doit employer un personnel hautement qualifié et spécialisé. «(…) On a une dame qui fait du risque de sécurité pour tout ce qui se rapporte aux risques associés aux pays étrangers, tout ce qui s'appelle «force» lorsque l'on va dans un pays étranger. (…) Y a aussi un type qui gère le programme de simulations. Ce gestionnaire ajoute qu'il bénéficie aussi d'un responsable des communications qui aide à pousser le message»[26].

Cette forme de structure décisionnelle et la présence de comités de gouvernance de la sécurité, se retrouvent au sein d'entreprises qui comptent de 7 000 à 30 000 employés. Le cas des PME, nous pouvons le deviner, est largement différent : une structure hiérarchique souvent aplatie, des moyens financiers plus limités, mais surtout, des besoins et des enjeux qui sont difficilement comparables. La gestion des risques informationnels en PME existe mais sa coordination nécessite moins d'intervenants. Pour l'application concrète de mesures de sécurité, six gestionnaires sur quinze (dont deux issus de grandes entreprises) nous ont avoués avoir pris eux-mêmes la décision.

[26] Comprendre : vendre les projets de sécurité et faire circuler l'information aux bonnes personnes.

Lorsque des projets de plus grande envergure sont envisagés, la décision se prend en groupe, souvent informel et organisé de manière provisoire.

> «C'est une discussion avec le v.-.p. opérations qui parle avec v.-p. r.-h.. Il y aura quelques échanges dans les deux sens; quels sont avantages et inconvénients. Et ensuite, le plan pourra être mis en place. Donc avantage de la petite structure. On lève les flags plus rapidement, on change les choses plus rapidement. À l'informatique, c'est mon ami, je l'appelle et on en discute sur-le-champ. Y a une capacité à se réajuster rapidement» (Interviewé 12).

Les propos de deux autres gestionnaires (Interviewés 3 et 4), l'un responsable des TI et l'autre responsable de la sécurité physique pour la même entreprise, abondent dans le même sens. Selon l'interviewé 3 : «À trois, on se complète bien (…) et je dirais qu'avec S, qui a le côté juridique, C qui a l'aspect sécurité plus physique et moi (…) c'est un peu mon dada de me préoccuper de la sécurité informationnelle». Cette synergie entre la sécurité dite «physique» et la sécurité de l'information ne se rencontre toutefois pas dans toutes les entreprises. Certains propos laissent même supposer que la sécurité physique serait obsolète, n'aurait plus sa raison d'être. Du moins, c'est ce que nous pouvons déduire des paroles de l'interviewé 5 :

> «Le volet "sécurité physique" c'est une barrière, il me faut une carte d'accès, c'est sûr y a toujours des lacunes (…) bon, j'vais arriver les bras chargés en veston-cravate et y a quelqu'un qui va m'ouvrir la porte. (…) Y savent même pas est-ce que j'suis un employé ou non. Pis ça, c'est dans toutes les entreprises. Par contre, si quelqu'un installe un router sans fil ici ben j'ai même pas besoin de rentrer dans la bâtisse pour accéder au réseau».

Ce même gestionnaire avoue que la communication entre les deux départements se limite au volet «enquête», c'est-à-dire, lorsqu'un délit est commis et que l'enquête nécessite l'implication des TI. «(…) On a des outils de forensique, pour analyser le

contenu d'un poste de travail même si on a pas le mot de passe, on a tout ce qui faut pour ça».

L'interviewé 8, qui a vécu une relation parfois houleuse avec le département TI, nous a quant à lui fait part de ses tribulations : «Parce que des fois, vous faites des choses, vous êtes concentré technique et vous pensez pas aux impacts sur l'entreprise, aux impacts sur la protection de l'information». Ce que ce gestionnaire nous dit, c'est que les ingénieurs ou techniciens en informatique manquent de perspective, leur intérêt démesuré pour l'acquisition de nouvelles technologies les rend aveugles face à la contrepartie que représentent les risques informationnels. Bien qu'il s'agisse d'un problème résorbé dans le cas de l'interviewé 8, cette fracture entre la sécurité physique et la sécurité informatique a été décelée dans les propos de deux autres gestionnaires (Interviewés 5 et 15).

Par ailleurs, certains interviewés (10 et 13) ont aussi mentionné que dans leur entreprise, il y a chevauchement entre les départements (sécurité informatique et sécurité physique) pour l'exécution de certaines tâches, notamment, les contrôles d'accès. D'autres responsabilités relèvent naturellement de l'un ou l'autre des départements et aucun chevauchement n'est envisageable comme par exemple, lorsqu'il est question d'enquêtes pré-emploi. Quant au code d'éthique, l'interviewé 10 précise que «chacun a son propre manuel et ses propres directives».

Il est néanmoins important de préciser que la relation entre le département de la sécurité physique et le département TI (ou sécurité de l'information) relève d'une toute autre dynamique lorsque l'implication d'acteurs externes influents accroit la nécessité d'avoir un système de communication en temps réel. Des liens de proximité étroits entre la sécurité physique et les TI ne sont alors plus une option mais une obligation (Interviewés 1, 2 et 8). L'impact d'une communication inadéquate ou défaillante dans certains cas particuliers, pourrait même avoir des conséquences allant jusqu'à menacer la sécurité de la population selon certains interviewés.

En résumé, nous remarquons que la gestion des risques informationnels passe par la mise en place de relations formelles et/ou informelles dont les principes de coopération et d'harmonie varient considérablement d'une entreprise à une autre. Le gestionnaire de la sécurité, dans une structure d'échange où chaque acteur se positionne au cœur d'un jeu de pouvoir et de contre-pouvoir, doit par ailleurs s'assurer qu'il ne sacrifie pas les objectifs de sécurité au profit d'autres objectifs. Rémi (1996), Blanc (2009) et Zwarterook (2013), dans leur description de la transaction sociale, ajouteraient qu'il s'agit de trouver des compromis acceptables sans pour autant céder sur les valeurs fondamentales[27] qui animent chacun des groupes ou des individus qui prend part à la prise de décision. Nous constatons aussi que la gouvernance de la sécurité de l'information implique des structures aussi diverses que les acteurs qui sont conviés à y participer. Comme l'entreprise évolue dans un environnement toujours en mouvement, ces structures de gouvernance sont appelées à se transformer au fil du temps, laissant présager du même coup que la fonction «sécurité» pourrait encore subir de profonds changements notamment en ce qui a trait à la protection du patrimoine informationnel de l'entreprise.

4.2.2 À l'externe : une question de nécessité

Le processus décisionnel de la gestion des risques informationnels suppose également une structure d'échanges où les interactions formelles et informelles se situent dans un contexte global où les acteurs externes représentent une pièce de l'engrenage essentielle au bon fonctionnement du mécanisme. Et lorsqu'il est question de la dynamique relationnelle externe, nous ne faisons pas exclusivement référence à la sous-traitance. En effet, en matière de gestion des risques informationnels, ce sont parfois les autorités publiques ou certaines instances gouvernementales qui sont impliquées, les firmes-

[27] Références aux valeurs organisationnelles telles que l'intégrité, la réputation, l'engagement, la confiance, l'éthique, le sens de la justice, le professionnalisme et la sécurité, pour ne nommer que celles-là.

conseils (vérifications, gestion des risques, systèmes d'information), les cabinets d'avocats spécialisés, les clients ou les fournisseurs pour ne mentionner que ceux-là.

À titre d'exemple, deux gestionnaires, pour des raisons sécuritaires et aussi, nous a-t-on avoué, pour des raisons de protectionnisme, entretiennent des relations privilégiées avec les services secrets, dont les pays ne peuvent être mentionnés ici. Cependant, la méfiance est toujours de mise selon l'expérience qu'en a fait l'interviewé 8 : «On se méfie toujours des gouvernements. Quand tu vas voir une agence gouvernementale, il te demande de l'information, il t'en donne jamais, c'est toujours pareil». Les interviewés 1, 2, et 4 nous ont aussi parlé de l'implication de certains ministères dont les responsabilités sont en lien avec les activités de l'entreprise. Ces mêmes interviewés nous ont aussi fait part de l'existence de partenariats formels et informels avec certains corps policiers. Poursuivant des objectifs relativement différents, ces gestionnaires nous ont dépeint leurs relations comme étant harmonieuses et réciproques en termes d'échange d'informations.

Par ailleurs, plusieurs gestionnaires se sont prononcés à l'effet que la sous-traitance de certaines activités devient inévitable. Discutons d'abord de la nécessité d'avoir recourt à une firme de vérificateurs externes. Dans la section précédente, nous avons abordé la question du respect des normes et des lois entourant par exemple, les processus de gestion des risques et la protection des données bancaires. Nous n'avons pratiquement qu'effleuré ces deux normes alors qu'il en existe une quantité faramineuse. «La vérification interne devient trop complexe, les risques sont trop grands et les attentes de la haute direction et du comité de vérification augmentent» (Stephen Hack, CPA, associé chez Ernst & Young)[28]. C'est pourquoi de nombreuses entreprises font appels aux services diversifiés de firmes comptables dont les activités s'étendent au niveau mondial. Comme nous l'avons souligné à quelques reprises, ces firmes se sont spécialisées dans la gestion des risques en entreprise : la sécurité des données et les risques technologiques en font partie.

[28] Propos recueillis par Scroppo, Fina. Version numérique de l'édition janvier-février 2006 de *CA Magasine*

> «Notre responsabilité, c'est d'embaucher une firme externe qui vient donner une opinion indépendante sur la sécurité des données. Nous on est sujet à une vérification de Sarbanes-Oxley, c'est une législation américaine parce que la compagnie a aussi des activités aux États-Unis. Et ça, ça audite ou vérifie, c'est toutes les règles de gouvernance, toutes les prises de décision à propos des données sensibles» (Interviewé 14).

Quant à la norme PCI, un gestionnaire, dont l'entreprise concentre ses activités au Canada, nous a appris que : «Lorsque quelqu'un est accrédité PCI, plus besoin d'inspection externe, c'est de l'auto-audit. Mais on doit rencontrer des normes strictes et ce sont des examens annuels pour renouveler la certification» (Interviewé 12).

Au total, huit entreprises de notre échantillon recourent aux services de vérificateurs externes pour la gouvernance des risques. Diverses raisons expliquent ce choix (si on peut l'exprimer ainsi), notamment une internationalisation des activités, un manque d'expertise à l'interne ou encore, une clause contractuelle (ce qui est souvent le cas avec les contrats gouvernementaux). Plusieurs de ces firmes de vérification possèdent également l'expertise dans une multitude d'autres domaines comme la gestion des TI et sont par conséquent, en mesure d'offrir des services tels que les tests d'intrusion. Ces tests consistent à tenter de pénétrer un système informatique et d'en découvrir les failles. Quelques-uns des gestionnaires avec lesquels nous nous sommes entretenus nous ont fait part qu'ils projettent de solliciter ce type de service d'une firme indépendante.

> «La seule chose c'est que bientôt on va se faire auditer, faire des tests de pénétration pour tout ce qui fait face à internet, nos sites (…). Parce que présentement, on le fait de l'interne, on scanne nos sites mais ça l'a une limitation, on y va vraiment ad hoc» (Interviewé 11).

La sous-traitance de l'expertise en TI est requise dans d'autres cas, notamment pour réévaluer le périmètre réseau : «On est en train de signer un nouveau contrat pour qu'il

fasse ce qu'on appelle le périmètre du réseau pour voir ce qui rentre et ce qui sort» (Interviewé 8) ou pour en redéfinir l'architecture : «On a mandaté une firme pour nous accompagner dans l'établissement de l'architecture du réseau, s'assurer que ça soit sécuritaire» (Interviewé 3). D'autres pensent même se tourner vers l'application en nuage : «(…) on est en train d'évaluer ce qu'il y a sur le marché pour ça. J'étais réticent au début mais de plus en plus il y a des compagnies qui sont sérieuses qui offrent des solutions qui sont blindées» (Interviewé 8). L'interviewé 5 quant à lui, possède l'expertise à l'interne alors il ne voit pas la nécessité de payer pour un service qu'il est en mesure de se procurer au sein même de son entreprise: «J'ai pris la décision parce que j'avais l'expertise à l'interne, sinon j'serais allé à l'extérieur». À cela, nous ajouterons les firmes d'avocats, qui fournissent aussi une expertise particulière au niveau de la protection des données et des renseignements personnels. Deux interviewés (8 et 12) nous ont mentionné avoir eu recours à une firme d'avocats pour «paramétrer» leurs actions en cette matière.

Par ailleurs, il est essentiel de souligner la présence de tierces parties qui, sans influencer directement le processus décisionnel du gestionnaire de la sécurité, représentent, et nous reprenons ici les termes de l'interviewé 10, «le maillon faible» de la chaîne : les clients et les fournisseurs. S'il est possible de choisir un autre fournisseur par crainte que celui-ci ne respecte pas nos standards de sécurité, il n'en est rien pour les clients. Ce que nous rapportent certains interviewés, c'est que bien que l'environnement de l'entreprise soit contrôlé contre toute intrusion inopportune (ou presque), l'environnement des clients et des fournisseurs demeurent inconnu. «Ils attendent que quelque chose arrive pour agir» (Interviewé 9). Cette affirmation reflète d'ailleurs l'une des préoccupations majeures des répondants de divers sondages que nous avons consultés. Comme la sous-traitance devient un moyen de plus en plus efficace pour avoir recours à une expertise particulière durant une période prédéterminée, il faut considérer que le degré d'exposition au risque augmente en conséquence de ce que l'organisation perd en termes de contrôle des processus de sécurité (Deloitte 2013). Dans le meilleur des cas, il sera possible de négocier une clause de confidentialité comportant certains paramètres liés à la sécurité de l'information.

Finalement, soulignons que malgré l'influence structurante importante que les assureurs peuvent avoir sur la gestion des risques en entreprise, aucun des sujets interviewés n'en a même fait mention. L'occasion s'est pourtant présentée à quelques reprises, notamment lorsqu'il a été question de contraintes, des acteurs externes ou des tierces parties. Nous aurions pu nous attendre à ce que les sujets membres d'un comité de gouvernance en face allusion mais cela n'a pas été le cas. Même du côté des PME, les assureurs n'ont jamais été mentionnés. Est-ce parce que les assureurs traitent directement avec le département légal ou le directeur général dans le cas des PME? Et bien que dans certains cas, le domaine d'activités de l'entreprise pourrait susciter moins d'obligations de la part des assureurs, d'autres ne pourraient y échapper. Quoi qu'il en soit, à l'heure actuelle, nous ne pouvons que spéculer.

En résumé, les relations qu'entretient le gestionnaire de la sécurité avec les autorités publiques, les firmes conseils, les bureaux d'avocats, les clients et les fournisseurs ne dépendent pas uniquement de la taille de l'entreprise et de sa capacité à engager des ressources compétentes. Les propos des interviewés nous convainquent que d'une part, la demande de services est fonction de la conjoncture et de besoins souvent provisoires et spécifiques. D'autre part, les activités de l'entreprise obligent les gestionnaires à s'engager dans un rapport de convenance afin d'assurer la réputation de l'organisation et la conformité aux lois et normes en vigueur mais aussi, dans certains cas, afin de protéger les intérêts de la population et par extension, ceux de l'État.

4.2.3 Réseaux

Pour mener à bien sa mission, le gestionnaire bénéficie généralement d'un réseau assez étendu de contacts personnels et professionnels sur lesquels il peut se fier. Si la plupart des interviewés sont membres à part entière de réseaux formels, d'autres n'en voient pas la nécessité.

> «Peut-être que si on était une petite entreprise et que j'étais seul dans ma gang, j'y penserais sans doute. Étant donné que c'est une grande corporation, moi je travaille en équipe avec les directeurs informatiques de chaque région. On partage nos expertises, les meilleures pratiques et dans le groupe, on s'assure que par sujet, il y a des gens qui seront formés à l'externe et qui vont ensuite se partager l'information, qui vont participer à des séminaires, des colloques» (Interviewé 14).

L'interviewé 11 nous confiait quant à lui qu'il n'est membre d'aucun réseau, formel ou informel et que dans l'entreprise (qui compte des milliers d'employés), il ne bénéficie de l'expertise d'aucun collègue de son niveau ou d'un niveau supérieur. Il ajoute ne pas en ressentir le besoin. Des quinze gestionnaires interviewés, il est le seul à avoir tenu ces propos puisque même au sein de PME, les gestionnaires sont soit membre d'un réseau professionnel, soit membre d'un comité ou les deux. Est-ce que cela s'explique par un désir de demeurer indépendant et complètement autonome ou encore, est-ce le fait d'avoir bénéficié des conseils d'un mentor pendant quelques années? La deuxième option nous parait la plus probable dans ce cas puisque le discours de ce gestionnaire laissait transparaitre une réelle admiration et un respect qui, semble-t-il, n'a pu être égalé par la suite. Ce cas particulier n'est cependant pas représentatif de l'échantillon puisque la majorité des gestionnaires sont membres de plusieurs réseaux professionnels et associations : CQCD, AQIS, ASIQ, ASIS[29], pour ne nommer que celles-là. La plupart d'entre eux s'implique dans le milieu de la sécurité par le biais de différentes activités: certains offrent de la formation, d'autres siègent sur divers comités, ils assistent à des colloques ou sont eux-mêmes conférenciers.

Pour une majorité d'entres eux, ancien policiers ou non, le réseau de contacts s'étend à tous les niveaux, de la scène politique au milieu policier en passant par les compétiteurs. «(…) On se sert beaucoup de nos contacts sur le marché faque on se tient informé, et quand on apprend des choses, on le communique» (Interviewé 5). L'interviewé 3,

[29] CQCD : Conseil québécois du commerce de détail; AQIS : Association Québécoise de l'industrie de la sécurité; ASIQ : Association de la sécurité de l'information du Québec; ASIS : American society for industry security.

gestionnaire d'une PME tient des propos similaires : «B a son réseau de contacts et ça aussi c'est une source d'informations importante. Des sources qu'il utilise une fois de temps en temps quand il n'a pas de réponse». Les contacts personnels occupent donc une place prépondérante lorsqu'il est question de sécurité de l'information et selon ce gestionnaire «la meilleure information provient des contacts personnels» (Interviewé 12).

Par ailleurs, au moins la moitié des interviewés nous ont mentionné faire partie de comités qui réunissent leurs membres pour discuter des tendances de l'industrie en matière de sécurité. L'interviewé 2 nous résume sa situation : «Moi, j'suis pas membre d'un réseau professionnel. Par contre on est membre de plusieurs comités. Des comités qui sont très importants pour développer les «trends» (tendance)». Le fait d'entretenir des liens avec des professionnels du milieu ou avec les membres de son organisation apporte donc son lot d'avantage. Non seulement, il s'y développe une meilleure connaissance des risques et des menaces potentielles mais l'information devient rapidement accessible. Bien que la situation de ce gestionnaire soit particulière, elle reflète néanmoins les privilèges d'un réseau organisé :

> «La circulation de l'information, c'est presque instantané, vous êtes au fait de tout ce qui se passe. Un inspecteur est en lien avec le ministère ABC puis aux États-Unis, G est responsable des liens avec les autres agences. Faque oui, c'est un gros network (…) quant y a quelque chose (…), on est tout de suite au courant, on augmente la sécurité (…)» (Interviewé 2).

Enfin, qu'il soit formel ou informel, le réseau de sécurité entraîne une plus-value au processus décisionnel du gestionnaire en matière de gestion des risques informationnels. Quatorze des quinze gestionnaires rencontrés partagent cet avis. L'un deux a par ailleurs ajouté que de toutes les sources d'information, le réseau professionnel demeure le plus pertinent : «Moi les sources d'informations sont à plusieurs égards mais je pense principalement au réseau professionnel avec qui tu transiges, les associations

professionnelles qui ont trait au métier dans lequel tu fais partie et que tu es actif, les échanges entre nous (…)» (Interviewé 10).

Les gestionnaires nous ont évidemment fait part qu'ils ont recours à d'autres sources pour s'informer quant aux risques informationnels. L'interviewé 5 nous parle des sites d'hackers et des sites de fournisseurs et précise «qu'on peut pas se limiter à une seule source». L'interviewé 11 affirme quant à lui que «s'abonner à des sites de sécurité» n'offrent aux gestionnaires «qu'une idée générale des vulnérabilités». Trois des quinze gestionnaires (spécialisés en sécurité de l'information) ont également mentionné avoir créé une vigie technologique et un autre nous a admis avoir acquis un logiciel d'extraction de données particulièrement puissant qui lui permet de mieux gérer les risques auxquels son organisation pourrait être exposée.

Nous pouvons dire que les réseaux représentent certes, un avantage pour les gestionnaires de la sécurité qui doivent veiller à la protection du patrimoine informationnel de l'entreprise. Cependant, la majorité d'entres eux s'entendent pour affirmer que le renseignement ne peut se construire qu'à partir d'une multitude de sources : données statistiques, tests, revues spécialisées, sites web, relations professionnelles, expérience et intuition, point sur lequel nous n'avons pas élaboré mais qui a été mentionné à quelques reprises par certains gestionnaires plus expérimentés voire même plus âgés que la moyenne. Retenons simplement que le processus de qualification et de quantification des risques jumelé à une dynamique relationnelle impliquant des principes d'échange d'informations et de connaissances poursuit un objectif commun inter-organisationnel de réduction des risques informationnels. Même si, à différents degrés, nous pouvons nous attendre à une certaine rétention de l'information qui pourrait être considérée comme plus sensible, il n'en demeure pas moins que l'organisation bénéficie directement de cette forme d'interactions entre gestionnaires de la sécurité. Dans la prochaine section, nous allons d'ailleurs tracer le profil de ces gestionnaires, ce qui nous permettra dans une section ultérieure, de mieux comprendre la dynamique relationnelle qui prévaut au sein de chaque organisation.

4.3 PROFIL DU GESTIONNAIRE

Aborder cet aspect de la recherche a suscité beaucoup de passion et de fierté de la part des gestionnaires interviewés. Nous nous sommes rendus compte qu'au sein de notre échantillon, l'âge a plus ou moins d'importance puisque la plupart des interviewés ont fait leurs premières armes à un très jeune âge et ont débuté tout en bas de l'échelle hiérarchique. Plus tôt, dans le chapitre traitant de la méthodologie, nous avons dressé un portrait de ces gestionnaires en tenant compte de leur fonction, du type d'industrie d'où ils sont issus, de leur expérience et de leur scolarité. Nous en ferons ici un court rappel. D'abord, notre échantillon compte 6 gestionnaires TI, 8 gestionnaires de la sécurité physique et un gestionnaire de la sécurité globale, c'est-à-dire qu'il occupe un poste qui chapeaute à la fois les TI et la sécurité physique. Parmi les quinze interviewés, deux ont débuté leur carrière comme policier alors que deux autres ont été militaires. Finalement, ils ont chacun un parcours académique assez diversifié : cinq d'entres eux ont au moins un diplôme d'études collégiales, huit ont obtenu un diplôme universitaire de 1er cycle (ou l'équivalent) et deux autres ont un diplôme universitaire de 2^{e} cycle.

4.3.1 Rôle et responsabilités

Leurs rôles peuvent se diviser principalement en deux catégories : les décideurs et les exécutants. Les premiers, que nous retrouvons majoritairement dans les PME, bénéficient d'un poste relativement élevé dans la hiérarchie. Ils ont la liberté de créer des projets, de prendre des initiatives mais surtout, ils ont la responsabilité de prendre des décisions. Pour d'autres, ils ont un rôle davantage passif au sein du processus décisionnel : ils s'assurent que les processus sont suivi de façon rigoureuse et que les mesures qui sont mise en place sont efficaces et efficientes : «Mon rôle est de participer aux initiatives d'un collègue américain qui lui est un leader, c'est notre officier en matière de sécurité de l'information et de sécurité sur les cartes de crédit» (Interviewé 14). D'autres ont un mandat beaucoup plus élargi. L'interviewé 2 nous explique en quoi consiste ses fonctions.

> «Notre but, c'est de s'assurer que du point A au point B, les marchandises soient correctes. Aussi, on agit comme «trusted advisor», c'est comme un «aviseur» de confiance. C'est la facette de recommandations. Nous autres, en tant qu'«aviseur» de confiance, on va aller chercher l'information pis on va dire voici ce qui faut que tu fasses, ce qui va falloir faire, parce qu'on a des contacts partout».

Nous pourrions croire que le transport de marchandises ne constitue pas un risque informationnel mais lorsqu'on s'y attarde, on se rend vite compte que le processus lié au transport, l'itinéraire des véhicules et le type de marchandises, pour ne nommer que ces éléments, sont des données sensibles et par conséquent, elles doivent faire l'objet d'une analyse de risques et être protégées. Notons que plusieurs des interviewés nous ont parlé de cette facette de leur travail qui consiste à recommander des solutions de sécurité à la direction. En parlant de ses responsabilités au sein de l'entreprise, l'un d'eux affirme que les problèmes qui surviennent nécessitent des solutions variées adaptées à chaque problématique et que parfois, une solution temporaire demeure la seule envisageable :

> «Si j'ai besoin d'élaborer une solution, bon ben, on va créer un «task force» et on va élaborer une solution rapide. Des fois, peut être…on va mettre un «plaster» en attendant pour limiter les dégâts, minimiser les risques mais entre-temps, on va trouver une solution permanente» (Interviewé 5).

Dans le commerce de détail, les rôles et responsabilités des gestionnaires sont fonction de la structure hiérarchique en place, de la culture informationnelle de l'entreprise mais avant tout, de la nature des activités de ces entreprises. Quatre interviewés (9, 12, 13 et 15) nous ont tenus des propos relativement similaires à ce sujet: «L'information qui doit être protégée, c'est toute la gestion de l'information entourant le crédit, l'information concernant la clientèle et aussi, au niveau des employés (…) des enquêtes et des arrestations» (Interviewé 12).

Nous pouvons constater que, de manière générale, les gestionnaires de la sécurité occupent des postes auxquels sont rattachées de multiples responsabilités. Certaines ne se rencontrent que dans les grandes entreprises comme la gestion du cyber-risque (interviewés 1, 5, 8, 11 et 14) alors que d'autres font partie intégrante de la fonction sécurité telle que nous la concevons. En effet, dans le cadre de ses fonctions, le gestionnaire de la sécurité procède à des enquêtes, élabore des politiques, conçoit des manuels de procédures, il identifie des problématiques récurrentes, s'occupe de la gestion des identités et des accès, gère des équipes de travail, il consacre du temps à la formation et à la sensibilisation des employés mais surtout, il recommande des solutions à l'organisation qui peut choisir d'en tenir compte ou non. Les propos des gestionnaires laissent néanmoins supposer qu'une même responsabilité ou tâche peut s'accomplir dans des conditions qui peuvent considérablement varier d'une situation à une autre. Par exemple, on peut être proactif en élaborant un programme de sensibilisation dont la mise en place s'échelonnera sur plusieurs semaines, voire même plusieurs mois. Par contre, un incident relatif à un bris de confidentialité implique une situation de gestion de crise qui, conséquemment, peut donner lieu à une sensibilisation massive et immédiate de milliers d'employés. L'application efficace d'une solution adaptée au contexte sera, dans un cas comme dans l'autre, facilitée par l'habileté du gestionnaire à formuler ses recommandations et par son capital social intra-entreprise.

Ajoutons finalement que les rôles et responsabilités des gestionnaires peuvent également variés en fonction de leur domaine d'expertise. Par exemple, l'instauration d'un programme de veille technologique ou de vigie (Interviewés 1 et 3) sera rarement l'initiative du gestionnaire de la sécurité physique de même que tout ce qui concerne l'installation de logiciels anti-virus, pare-feu, etc. Pourquoi? «C'est le gars de l'informatique qui s'occupe de ça!» (Interviewé 10). Pour ce qui est de la portion «enquête», cette responsabilité sera attribuée, dans près de 70% des cas, au gestionnaire de la sécurité physique auquel s'ajoute une collaboration étroite de la part du gestionnaire TI dans tous les cas. L'enquête forensique est quant à elle réalisée, la plupart du temps par une tierce partie. Il est cependant intéressant de noter que lorsqu'il est question de la gestion des risques informationnels liée à l'utilisation des nouvelles

technologies de communication, les préoccupations sont les mêmes et les discours se rejoignent de parts et d'autres.

En résumé, qu'il s'agisse d'un gestionnaire TI ou d'un gestionnaire de la sécurité physique, chacun est conscient des enjeux globaux propres à son organisation. Évidemment, sur le fond comme sur la forme, il y a des différences notables quant aux moyens de prévenir ou de réduire le risque mais nous y reviendrons plus tard. Les rôles et responsabilités sont toutefois relativement similaires si nous excluons certaines considérations techniques qui, sans être évitées, relèvent d'une expertise que le gestionnaire avisé saura se départir judicieusement.

4.3.2 Cheminement de carrière

Comme nous l'avons souligné dans la section précédente, les gestionnaires interviewés possèdent pour la plupart, un important capital social et de nombreuses années d'expériences dans leur domaine respectif. Même pour les plus jeunes, nous parlons de quinze à vingt ans à gravir les échelons dans le domaine de la sécurité, se faire une place parmi les plus expérimentés et se bâtir une réputation. La plupart d'entres eux bénéficient de plus, d'un bagage de connaissances diversifiés, acquis au sein de différentes organisations. Ils ont été témoins d'évènements critiques qui ont bouleversé le monde de la sécurité. «(…) J'connais le risque en maudit par exemple (…). Pis dans l'armée j'en ai vu des choses arriver pis dans ma vie, j'ai vu des choses arriver en masse» (Interviewé 8). Ils ont aussi dû s'adapter à l'évolution rapide de la technologie :

> «J'ai travaillé comme développeur, comme consultant, j'ai fait un peu de tout. J'ai commencé à une époque où il n'y avait pas beaucoup d'informatisation. (…) Moi, j'ai eu l'occasion de voir l'évolution des différentes technologies (…) mais aussi l'évolution de toutes les sortes de virus. Ça a pris des «crashs», des intrusions majeures dans les systèmes des grandes entreprises, dans les universités, à la NASA pour que le monde

> commence à s'éveiller plus à ça. J'ai été confronté à ça au fil des années alors pour moi les données, c'est quelque chose d'une très grande valeur autant pour son intégrité que pour sa confidentialité» (Interviewé 14).

Un autre gestionnaire mentionne quant à lui : «c'est sûr que plus on a de l'expérience, plus que, si on veut, on est réaliste, on prend des décisions plus éclairées» (Interviewé 11). Les propos des quinze interviewés sont sans équivoque : l'expérience qu'ils ont acquise revêt une valeur sans égal qui ne peut être compensée par aucune formation académique, de quelque niveau que ce soit. «Sans avoir l'expérience, c'est un peu difficile de connaître le milieu (…). Moi, un jeune qui finit son bac pis qui s'en va faire un MBA tout suite, j'trouve qui a pas de plus-value à ça» (Interviewé 2). Certains gestionnaires (2, 5, 9, 11 et 14) ont fait référence aux jeunes universitaires qui tentent de s'intégrer dans le milieu de la sécurité en faisant valoir leurs acquis théoriques et en visant un peu trop hâtivement le sommet de la hiérarchie. «(…) c'est l'intuition…j'les «size» ces personnes là. Tu vois quand quelqu'un veut juste monter. Moi, j'ai toujours été dans l'industrie. Pas en suivant la vague. Tsé, j'ai jamais espéré…j'suis arrivé…on dirait que j'ai fait mes classes pis mon chemin à moi» (Interviewé 11). En sécurité de l'information, on les qualifie parfois même «d'extrémistes», c'est-à-dire par exemple, qu'ils ne jurent que par un seul type de logiciel ou qu'ils n'acceptent aucun avis ou aucune solution qui pourraient déroger à leur idéologie: «(…) des fois, ça amène des confrontations puis faut surtout pas aller dans cette direction-là! Faque oui, j'ai beaucoup de coaching à faire auprès de mon équipe, changer leur façon de voir les choses, on y va graduellement mais y a encore place à amélioration» (Interviewé 5).

Les études universitaires apportent néanmoins quelques avantages comme le souligne l'interviewé 11 qui, lors de notre rencontre, s'apprêtait à débuter un doctorat : «(…) pis qu'est-ce que je trouve que les études ont amené, c'est d'être capable de critiquer tous les côtés, de voir l'ensemble de la situation». Il mentionne également que les études aident à développer un esprit critique et à bien argumenter. Un second gestionnaire mentionne que son cheminement de carrière lui a pour sa part, permit d'acquérir cette vue d'ensemble : «(…) d'un point de vue management (…), mon approche est toujours :

bon, c'est beau là, t'es face à un arbre mais avant d'abattre l'arbre, où est-ce que tu t'en va, c'est quoi l'ampleur. C'est le recul, avoir une vue d'ensemble» (Interviewé 5). Nous avons aussi pu nous entretenir avec deux gestionnaires de la sécurité qui, selon leurs propos, jouissent d'un avantage non négligeable : celui d'avoir vécu l'expérience policière avant de se lancer dans la sphère privée de la sécurité :

> «C'est toutes les expériences que t'as passé à travers. Forcément, les aventures et les expériences de vie dans le domaine policier sont une excellente forme d'expérience pour apprendre. J'ai quitté, mais les choses que j'ai apprises dans ces deux endroits-là ont toujours été une plate-forme, une fondation très solide. Je suis capable de faire des relations lorsqu'on travaille avec les policiers, je suis capable de faire l'équilibre des choses» (Interviewé 10).

Quant au second gestionnaire (12), il semble particulièrement comblé par son cheminement de carrière. Après avoir été policier, il a enseigné à ses pairs pour ensuite s'impliquer activement dans l'entreprise privée : création de programmes de prévention, formation et rédaction de politiques de sécurité. Ce dernier nous explique que c'est une combinaison entre son expérience policière et son expérience en entreprise qui lui a permit d'occuper le poste où il se trouve aujourd'hui :

> «Si j'avais été que policier, on m'aurait pas engagé parce que quand tu veux identifier des problèmes et trouver des solutions, faut que tu ailles au cœur des entreprises et cela permet de voir les bons et les mauvais côtés. Et il faut que tu sois en mesure de livrer des choses concrètes et la formation qui va avec» (Interviewé 12).

L'expérience amène aussi, selon les gestionnaires interviewés, une certaine forme de respect, une «certaine crédibilité auprès de ses pairs» (Interviewé 2), particulièrement lorsque le gestionnaire en question a gravi les échelons au sein de l'entreprise pour laquelle il œuvre depuis des années.

> «Pis moi, (…) ça fait pas longtemps que j'suis en poste. J'suis chef d'équipe depuis début janvier. Avant ça, j'étais un analyste en sécurité pis (…) j'ai travaillé avec beaucoup d'autres employés, de différents départements pis c'est sûr que ça contribue à la maturité de quelqu'un vis-à-vis la sécurité».

Ce gestionnaire est le seul des quinze interviewés à avoir mentionné qu'il avait bénéficié, pendant quelques années des conseils d'un mentor, auparavant policier. Il ajoute qu'une grande part des décisions qu'il prend aujourd'hui est attribuable à ce mentorat. Un autre gestionnaire nous explique par ailleurs que son expérience, principalement dans le domaine de la sécurité de l'information, facilite la communication avec ses subordonnés et ses collègues : «Comme mon background est très TI (…) et le fait d'avoir travaillé dans des champs très techniques ben aujourd'hui les gens techniques me parlent pis j'comprends. (…) ça m'aide à mieux qualifier les risques» (Interviewé 5). Dans un même ordre d'idée, l'un des interviewés (8), reconnu pour son franc parler, nous explique qu'il ne ressent aucune gêne à présenter les risques, quels qu'ils soient «(…) moi je suis chanceux, je viens des TI alors ils m'ont connu pendant cinq ans, ils savent comment je suis, ils savent que je «drive» pas mal (…). Que ça vous plaise ou non, voici les risques!»

Ce que nous avons remarqué de ces entretiens, c'est d'abord, que l'expérience, les compétences techniques et les connaissances du «terrain» méritent le respect et assurent une certaines crédibilité au près des pairs. Rappelons que selon les travaux recensés par Kermish (2012), ces éléments constituaient également des facteurs organisationnels susceptibles d'influencer l'analyse multidimensionnelle des risques et par conséquent la gestion de ces mêmes risques. L'éducation en revanche, est présentée comme étant plus accessoire et ne semble être un avantage que lorsqu'elle est acquise par celui qui a commencé au bas de l'échelle, qui a fait ses preuves et qui a su mériter ses gallons. Notons aussi que les interviewés se distinguent les uns des autres quant à leurs champs de compétences. Notre échantillon compte 6 gestionnaires dont l'expertise est presque exclusivement relative au domaine de l'informatique. Comme nous avons pu le constater, leur discours traduit la facilité que ces derniers peuvent avoir à communiquer

l'information à des tiers et à comprendre le langage technique. Nous pouvons en conclure que même si la sécurité de l'information revêt une importance assez comparable chez l'ensemble des sujets, des différences subsistent quant à la maîtrise de certains outils visant à prévenir les risques informationnels, objet d'intérêts de la prochaine sous-section.

4.3.3 De quels outils disposent-ils?

Nous disions que la richesse d'une expérience variée, c'est-à-dire, acquise au sein de différentes organisations favorise l'adoption de comportements proactifs qui profitent à l'ensemble de l'organisation. Nous avons remarqué, suivant les propos des gestionnaires interviewés, que la plupart des politiques et procédures de sécurité qui ont été instaurées au sein de l'entreprise proviennent d'initiatives du gestionnaire de la sécurité. Indépendamment de la taille de l'entreprise, les mesures de sécurité mises en place pour protéger le patrimoine informationnel des organisations varient grandement d'une organisation à une autre même si certaines mesures se retrouvent dans la totalité des entreprises, comme le contrôle d'accès ou la gestion des identités. Nous serions aussi porté à croire qu'une majorité d'entreprises se sont munies d'un code d'éthique ou d'un guide de procédures relativement à la protection de leur patrimoine informationnel mais nous nous sommes rendu compte que près de la moitié d'entres elles n'en possédaient pas, faute de temps ou faute du gestionnaire de la sécurité qui n'en voit pas la nécessité. «Non, nous on n'en a pas, pas de manuel, pas de code de conduite (…)» (Interviewé 14). L'interviewé 4 nous mentionne quant à lui, qu'ils ont l'intention d'en produire un mais pour le moment «tous les gens qui ont une carte d'accès, une clé contrôlée, un code d'alarme, signent un consentement comme quoi ils sont propriétaires de ces codes-là entres autres, pas les passer, les partager ou quoi que ce soit». La signature d'un document qui engage le signataire à respecter certaines règles relativement à la confidentialité de l'information est une mesure que nous retrouvons effectivement dans la plupart des entreprises. Il faut toutefois préciser que dans la majorité de cas, il s'agit d'une politique de confidentialité qui se résume à quelques lignes et qui n'est

communiquée qu'au moment de l'embauche de l'employé comme le précise l'interviewé 11 : «Moi j'ai signé un code de conduite quand j'suis arrivé ici» ainsi que l'interviewé 12 : «(…) il y a signature de documents par les employés à l'embauche au niveau des politiques de confidentialité. Tout le monde doit signer un document sur la gestion informatique».

D'autres n'en sont pas à leurs premiers balbutiements au niveau de la protection du patrimoine informationnel. Certains en sont même à leur deuxième version du code d'éthique: «Y a un code d'éthique qui existe (…) on a une nouvelle version qui est sortie la semaine dernière puis y a un grand volet de confidentialité de l'information» (Interviewé 5). Deux des gestionnaires avec qui nous nous sommes entretenus ont poussé l'exercice encore plus loin. Le premier nous fait part que : «Toute la manière dont nos choses sont configurées vont être décrites là-dedans avec les standards de classifications des actifs informationnels (…)» (Interviewé 11). Le second nous mentionne qu'au sein de son entreprise, ils ont «une véritable politique de classification de l'information, totalement transparente, facile à comprendre. Et qui a tenu en cours de route» (Interviewé 8). Bien que seulement deux gestionnaires nous aient parlé de la classification des actifs informationnels, d'autres (interviewés 3, 4, 5, 7, 9, 10, 12, 13 et 15) ont discuté de la nécessité de compartimenter l'information afin de réduire les risques. En compartimentant l'information, il est ainsi possible de restreindre l'accès par groupe ou par département. Certains considèrent la compartimentation de l'information comme une mesure de prévention relativement simple à implanter et à maintenir. Cette mesure permet de réduire considérablement le risque de fraude et d'espionnage et si le vol de données est toujours possible, ces mêmes données, extraites de leur contexte sont dépouillées de leur sens et n'ont plus la même valeur.

D'autres moyens ayant été évoqués lors de nos entretiens relèvent de principes fondamentaux en sécurité de l'information. En effet, près de la moitié des gestionnaires interviewés, principalement les spécialistes des systèmes d'information nous ont parlé de quatre principaux critères à respecter lorsqu'il est question de la protection des données : la confidentialité, l'intégrité, la disponibilité et la traçabilité. Bien que ces critères se

doivent d'être intégrés à la gestion des systèmes d'informations, il s'agit aussi d'inciter l'employé à adopter un comportement responsable : éviter de partager ses mots de passe, demander les autorisations nécessaires avant de modifier ou de détruire des données ou s'assurer que l'information soit accessible en temps et lieu aux utilisateurs autorisés. Dans une entreprise qui œuvre dans la recherche et le développement, il devient toutefois très difficile de compartimenter l'information et de déterminer ce qui est confidentiel et ce qui ne l'est pas. On mise alors sur la sensibilisation:

> «On sensibilise tout le monde également. On laisse un flou quant à la sensibilité de l'information. Dans ce type de boîte, tout le monde, à un moment donné, aura de l'information confidentielle entre les mains. Donc, c'est mieux qu'ils fassent toujours attention» (Interviewé 6).

La sensibilisation est en effet un outil ou plutôt un moyen important dont se servent plusieurs gestionnaires dont l'objectif est de diminuer le risque à la source:

> «Nous, on a commencé une initiative où on envoie un petit bulletin. On va envoyer un petit bulletin chaque semaine par rapport à la sécurité de l'information pour éduquer les gens par rapport à l'usage des mots de passe, la complexité des mots de passe, où devrait résider l'information, un peu de tout. On est au tout début de ce processus-là» (Interviewé 14).

De plus, lorsqu'il est question de réduire le risque à la source, les interviewés 3, 4, 10 et 12 nous ont confiés que la vérification pré-emploi (état du crédit personnel et antécédents criminels) est définitivement une nécessité. L'interviewé 10 ajoute que les mesures d'embauche sont un élément essentiel du processus de gestion des risques informationnels : «Nous, on engage des gens à qui on donne une certaine confiance, on met un encadrement».

À cela, s'ajoutent des outils techniques comme le chiffrement des données sur les portables : «Faque les personnes qui ont soit des données confidentielles, soit des choses

sensibles se font installer ça. C'est un «no-brainer», y sont obligés» (Interviewé 11). Un autre ajoute que «(…) si quelqu'un venait à le voler, il aurait besoin, en plus de la clé «d'encryption», trois mots de passe, situés à différents niveaux dans le système». Ce gestionnaire nous précise toutefois qu'il s'agit d'une décision personnelle et que ce n'est pas tous les ordinateurs portables appartenant à l'entreprise qui sont munis d'une clé de chiffrement.

On nous fait part également d'activités de surveillance active appliquées sur tous les types d'appareils électroniques (Interviewé 8) et de la production de rapports de sécurité quotidiens (Interviewés 1, 2, 5, 11 et 14) : «(…) on a un opérateur en sécurité qui lui, passe justement le début de sa journée à tout valider les contrôles qu'on a en place» (Interviewé 11). Réduire le risque à la source permet effectivement de diminuer le nombre d'interventions. L'interviewé 14 nous fait remarquer «qu'il y a des contraintes mais aussi des avantages à se servir d'outils, à «monitorer» des événements, à restreindre les accès, parce qu'on passerait beaucoup plus de temps à réparer que le temps qu'on investit à se protéger». Par ailleurs, pour une entreprise dont les risques se chiffrent par centaines, il est aussi question d'exercices de simulation d'incidents en temps réels et, pour les déplacements à l'étranger, d'utilisation d'ordinateurs portables dont les données ont préalablement été effacées (Interviewé 8).

Si certains de ces outils nécessitent un budget plus imposant, d'autres (comme la vérification pré-emploi et la sensibilisation) sont davantage considérés comme des mesures de prévention «de base», selon une majorité de gestionnaires interviewés. L'un de ces gestionnaires nous dresse un résumé de ce qui, selon lui, devrait être privilégié dans une organisation :

> «Ça prend à l'entreprise une volonté de le faire, faut que t'ais un encadrement général sans être trop spécifique parce que quand t'entre dans le trop spécifique, c'est là que t'as un débordement pis que t'as de la difficulté à faire ce que t'as à faire. Bon éthique de travail, un bon leadership et puis évidemment de la formation à tes employés. Le point suivant, c'est les

> mesures d'embauche; tu t'assures que lors de l'embauche tu fais les vérifications que tu as à faire et tu t'assures aussi que les gens que tu engages sont avisés de l'importance de l'information, de la classification de l'information. Et puis après ça c'est toute une attitude de suivi et de contrôle au fur et à mesure. Dans ce temps-là, tu évites le débordement, le 'dérapement'» (Interviewé 10).

Au cours de nos entretiens, nous avons pu constater que les gestionnaires qui s'impliquent dans le milieu de la sécurité, sont davantage proactifs et font preuve de plus d'initiative lorsqu'il est question de gestion des risques informationnels. L'exception à la règle demeure l'interviewé 11 qui bien qu'il ne fasse partie d'aucun réseau professionnel ou de comité (formel ou informel), a toutefois eu le privilège d'avoir un mentor; ce qui explique peut-être la raison pour laquelle il se démarque dans la mise en place de procédés et de politiques de sécurité. Il est également important de noter que la mise en place de mesures innovantes et de politiques rigoureuses visant à protéger le patrimoine informationnel des organisations sont généralement adoptées par les gestionnaires TI. L'âge est cependant un facteur quant aux choix des solutions adoptées par ces derniers. Bien que nous n'ayons pas eu l'occasion d'interviewer de jeunes gestionnaires en considérant «jeunes» les individus âgés de moins de trente ans, le choc générationnel est un sujet qui nous a été rappelé à maintes reprises et ce, tant chez les gestionnaires de la sécurité physique que chez les gestionnaires TI. L'achat d'outils techniques dispendieux semble être le premier réflexe chez les subordonnés les plus jeunes alors que les gestionnaires plus expérimentés sans exclure les outils techniques, optent pour des mesures à long terme qui intègrent les aspects humains, financiers, légaux, opérationnels et technologiques. Soulignons finalement qu'indépendamment des domaines d'expertise, le discours des gestionnaires nous apprend que les solutions aux problèmes de sécurité sont davantage orientés vers la prévention et la sensibilisation des employés à la sécurité de l'information. Conscients de la difficulté, voire même de l'impossibilité à contrôler tous les risques liés à l'utilisation des nouvelles technologies, les gestionnaires consacrent désormais plus d'efforts à promouvoir, à informer et à sensibiliser les employés aux risques informationnels.

Ce constat rejoint les conclusions de l'étude Rhee, Ryu et Kim publiée en 2012 dans Computer & Security. Les auteurs mentionnaient à ce sujet : «(…) information security done right should consider not only technical dimensions but also, human factors» (p.30). Cette tendance se remarque également dans l'industrie[30] qui reconnait que le comportement de l'employé représente l'une des principales vulnérabilités de l'organisation en termes de sécurité de l'information. Il semble en effet que les gestionnaires de la sécurité se soient éveillés à une problématique majeure qui consistait à donner des «réponses technologiques à des problèmes humains» (Ghernaouti-Hélie 2007).

4.4 IDENTIFICATION ET HIÉRARCHISATION DES RISQUES

Maintenant que nous avons décrit comment les aspects contextuels, relationnels et personnels influencent la manière dont la gestion des risques se déroule, nous aimerions nous pencher sur deux éléments qui nous sont apparus ressortir de manière particulièrement importante lors des entrevues : le processus d'identification et de hiérarchisation des risques (l'un de nos objectifs spécifiques), et la difficile conciliation entre les intérêts sécuritaires et la profitabilité de l'entreprise.

En effet, nous pouvons affirmer que le processus de gestion des risques dépend d'un nombre important de facteurs, tant contextuels que relationnels. Pour ces raisons, le processus d'identification et de hiérarchisation des risques relève d'un exercice qui doit constamment être revu et corrigé. «J'te dirais que c'est tout le temps un processus qui est à revoir, à refaire» (Interviewé 2). Dans le commerce au détail par exemple, l'analyse de risques est encore loin d'être systématique et la hiérarchisation des risques dépend en grande partie de la culture informationnelle en place ainsi que des initiatives entreprises par le gestionnaire de la sécurité. En matière de gestion des risques informationnels, ces derniers s'entendent toutefois pour dire que ce qui constitue, semble-t-il, le plus grand

[30] Sondages annuels de PricewaterhouseCoopers, Deloitte et Ernst & Young relativement aux risques informationnels (2010 à 2013).

risque, est sans contredit le vol de données à partir de cartes bancaires (cartes de débit et cartes de crédit). Récemment (la période diffère d'un gestionnaire à un autre), on remarque cependant un changement dans la manière de gérer le risque dans le secteur du commerce au détail: «Avant, certains risques ne se voyaient pas ou alors moins. On acceptait la perte «mystère», donc le risque car la source demeurait inconnue. Maintenant, on identifie mieux le risque, on accepte moins les pertes et on en parle» (Interviewé 12).

Nous avons aussi constaté au cours de nos entretiens, que les méthodes pour évaluer le risque varient grandement d'une entreprise à une autre. Cependant, la plupart des gestionnaires interviewés utilisent une approche combinant les analyses qualitatives et quantitatives. Par qualitative, on fait principalement référence à des échelles de classification de type descriptif à trois ou cinq niveaux, allant de «risque non significatif» à «risque très élevé». Même s'il s'agit de démarches standardisées, certains facteurs d'ordre contextuel et/ou relationnel viennent parfois influencer l'évaluation des risques. Si certains dossiers "brûlants" pouvant par exemple affecter la réputation de l'entreprise nécessitent une attention immédiate, d'autres risques disons-le, moins prioritaires, devront faire l'objet d'une réévaluation ultérieure. «Si le risque est moyen, on va doser. On va peut-être essayer de l'adresser mais on va regarder est-ce qu'y a un projet au cours de l'année qu'on pense qui va pouvoir toucher à ce volet là et si oui, ben on va l'adresser dans le projet en question» (Interviewé 5). Même lorsque certains risques importants sont identifiés, si ceux-ci peuvent être contrôlés par des mesures temporaires, des projets à plus long terme seront initiés. Ces projets, pouvant se dérouler sur une période allant de trois à cinq ans, demandent temps et investissements et sont répartis en plusieurs phases. Ce que nous constatons auprès des interviewés, c'est que malgré une technologie qui évolue rapidement, la mise en place de procédures ou de nouvelles méthodes de contrôle peut se traduire par un processus long et fastidieux. Toutefois, lorsqu'il est question de risques liés à des obligations légales, règlementaires ou contractuelles, la plupart des gestionnaires s'entendent pour dire qu'il s'agit de cas hautement prioritaires.

Les échelles quantitatives sont quant à elles beaucoup plus complexes et laissent peu de place à la subjectivité : il est question notamment de l'élaboration de scénarios de risques et de modélisation mathématique. L'un des gestionnaires interviewés nous a par ailleurs admis que selon lui, il y a très peu d'entreprises qui n'utilisent que la méthode quantitative : «C'est pas réaliste de ce que j'ai vu sur le marché à date» (Interviewé 5). Nous avons en effet pu constater que l'analyse qualitative demeure largement utilisée par les gestionnaires de la sécurité. Toutefois, lorsque les risques deviennent trop nombreux et que la matrice de risques se complexifie, la méthode quantitative n'est plus une option, comme nous en a fait part l'interviewé 8 :

> «(…) on a entrepris ce qu'on appelle un cyber risque deep dive. C'est-à-dire qu'on a fait une analyse de risque en profondeur de tous nos secteurs d'activités qui touchaient à la gestion de l'information pour savoir où on était à risque. Au bout de 18 mois, on a dit : il manque des risques dans votre matrice. On aura ajouté 47 risques dans la matrice. Alors, ces risques-là se sont retrouvés en addition à la matrice de risques qu'on avait élaborés. On a une matrice cinq par cinq».

Les gestionnaires nous ont aussi mentionné qu'ils comptent sur la fiabilité des rapports remis par les auditeurs internes et/ou externes en matière d'identification et de hiérarchisation des risques:

> «Eux vont auditer tes systèmes, vont faire des rapports. Pis là moi dans le fond, c'est là que j'entre en jeu. Quand les rapports arrivent, on me les donne, pis là on me dit « gères ça!» (…) parce qu'un auditeur va te donner une note par exemple, bon, moyen, mauvais, extrêmement mauvais» (Interviewé 11).

Bien que ces rapports soient essentiels au bon fonctionnement du processus de gestion des risques, certains interviewés nous ont admis que les recommandations des auditeurs sont parfois irréalistes et ne tiennent pas compte de la multitude d'acteurs qui

interviennent dans ledit processus ni des objectifs de l'entreprise en matière d'efficacité organisationnelle et de profitabilité. Les propos de ce gestionnaire résume bien cette situation : «Je sais interpréter ce qu'ils disent et moi, je sais la réalité, j'sais c'est quoi l'implication ou si on veut, le travail qu'il y a à faire pour mettre en place ce qui nous manque. Parce que souvent, eux-autres, y ont des objectifs qui sont peu réalistes» (Interviewé 11).

Est-ce que cette divergence constitue un obstacle à la gestion des risques informationnels ou assistons-nous à une forme de négociation où il est question de faire des compromis sur certains éléments au «meilleur intérêt de chacun» (Rémy 1996, p.13)? En fait, nous avons noté au fil des entretiens que l'identification et la hiérarchisation des risques relèvent d'un processus où les transactions sociales sont omniprésentes, à différents niveaux, forçant une modification du contexte, conséquence des interactions, des objectifs poursuivis et ultimement, des décisions qui sont prises. Ainsi, à travers l'analyse multidimensionnelle des risques, s'imbriquent, de manière parfois chaotique comme nous avons pu le constater, ce jeu d'acteurs d'où émergent des solutions qui, loin d'être parfaites, conviennent à toutes les parties jusqu'à ce qu'un nouvel élément s'ajoute et que le processus redémarre.

4.5 PROFITABILITÉ DE L'ENTREPRISE ET SÉCURITÉ : OBJECTIFS INCONCILIABLES?

Revenons sur cette dichotomie entre les objectifs poursuivis par l'entreprise et les objectifs de la sécurité puisqu'il s'agit d'un sujet qui a été abordé à maintes reprises par l'ensemble des gestionnaires de la sécurité avec lesquels nous nous sommes entretenus : «(…) la sécurité est pas là pour bloquer la business. Moi, jamais jamais j'vais le faire» (Interviewé 11). Les propos de l'interviewé 5 abondent aussi dans ce sens : «En théorie, faut pas faire ça! Oui mais la réalité en entreprise, c'est autre chose. J'peux pas empêcher les magasins de vendre!». Nous avons remarqué qu'au sein de notre échantillon, le discours des gestionnaires représente assez fidèlement l'évolution constatée à travers les

études d'envergure réalisées au cours des cinq dernières années par les firmes Deloitte, Ernst & Young et PricewaterhouseCoopers. L'un des gestionnaires interviewés (Interviewé 6) s'est par ailleurs vu étonné mais aussi ravi qu'un nombre grandissant d'acteurs de la sécurité s'éveille à la complexité organisationnelle et à la nécessité pour le gestionnaire de la sécurité d'être conscient de la finalité économique d'une entreprise. Les propos de l'Interviewé 12 sont en effet révélateurs de ce changement :

> «Avant d'amener un projet de l'avant (…), il faut que tu sois conscient de l'étape dans laquelle l'entreprise se trouve, de son contexte organisationnel. Si l'entreprise concentre ses efforts sur le développement de nouveaux marchés, ce n'est pas le bon moment pour présenter un projet de grande envergure. Qui plus est, il faut être préparé, avoir un plan bien défini. Il faut être stratégique dans son approche».

Ce que nous constatons, c'est que non seulement le gestionnaire de la sécurité intègre les notions de contexte organisationnel et de profitabilité à sa façon d'aborder la sécurité mais il y perçoit aussi l'opportunité de démontrer que la sécurité de l'information ne doit pas être considérée uniquement comme une contrainte. La promotion de la sécurité passe par la valorisation de ses avantages, comme un moyen de diminuer les pertes et par conséquent, de maximiser le profit. Comme nous l'a fait remarquer l'un des gestionnaires interviewés : «Mon but, c'est : qu'est-ce que j'dois mettre en place pour qu'ils puissent le faire? C'est mon approche. Faque de cette façon là, je me positionne et en même temps, je diminue les risques et tout le monde est content» (Interviewé 5). L'interviewé 14 nous mentionne quant à lui qu'il est «toujours plus facile d'obtenir du budget pour améliorer quelque chose qui va avoir un impact sur la business».

Comme en témoigne les propos de plusieurs gestionnaires, si l'organisation souhaite maintenir un niveau optimal d'efficacité, certains projets se doivent d'être réalisés et cela, malgré la présence d'un nombre parfois important de risques. Dans la mesure où le gestionnaire de la sécurité est impliqué dans ce type de projet, il pourra justifier son

implication et la plus-value de ses recommandations de plusieurs manières: «T'es obligé de le payer faque y as-tu quelque chose qu'on peut faire, on peux-tu être meilleur là-dedans? En mettant ça, oui on paye plus d'un million à la banque mais on s'est aperçu qu'on sauve 2 à 3 millions par année» (Interviewé 2). Si les efforts déployés à promouvoir la sécurité servent les intérêts économiques de l'entreprise, ils contribuent également à faciliter le processus de gestion des risques :

> «Ça veut dire, un seul mot de passe à se souvenir, y vont être plus efficaces, plus productifs. Donc, oui y faut sécuriser mais aussi, si c'est fait de la bonne façon, j'peux amener de quoi qui va les aider, qui va amener de la valeur. Mais pour moi, ça va me servir parce que ça va être plus sécuritaire» (Interviewé 5).

Évidemment, aucun des interviewés n'a affirmé que les projets étaient acceptées à l'unanimité car, faut-il le rappeler, la mise en place de procédures ou l'intégration de nouveaux outils sont présentés, la plupart du temps, sous forme de recommandations au comité de gouvernance ou aux membres de la direction de l'entreprise[31]. L'interviewé 1 nous racontait justement qu'au sein de son entreprise, les unités d'affaires sont responsables de leurs profits. S'ils ont une tolérance au risque élevé et qu'ils jugent qu'une somme de «500 000$» est mieux investie dans un projet de marketing, la décision finale leur revient et ce, malgré les doléances du gestionnaire de la sécurité et malgré les arguments qu'il apportera, aussi solides soient-ils. Et comme le renchérit l'interviewé 2, «On fait des recommandations : y en a qui sont suivies, d'autres qui sont un peu moins suivies (…)».

L'analyse de ces discours nous permet de déduire que les gestionnaires de la sécurité (qu'ils soient issus des TI ou de la sécurité physique) ont su adopter un style de gestion qui s'apparente à l'approche dite de la contingence (Donaldson 2001, Pennings 2013). C'est-à-dire qu'ils ont su se créer une place au sein du processus de gestion des risques

[31] La gestion quotidienne de la sécurité de l'information est exclue de ce processus

informationnels non seulement en tenant compte des particularités du contexte mais aussi en fonction des objectifs plus généraux de l'organisation, tangente qui se remarque aussi au sein de l'industrie de la sécurité de l'information[32]. Il faut toutefois admettre que les stratégies adoptées pour protéger les actifs informationnels de l'entreprise se traduisent bien souvent en compromis fragiles et provisoires et la solution qui parait optimale d'un point de vue financier ou opérationnel ne l'est peut-être pas d'un point de vue sécuritaire.

5. LA GESTION DES RISQUES INFORMATIONNELS À TRAVERS DEUX APPROCHES : LA TRANSACTION SOCIALE ET L'APPROCHE MULTIDIMENTIONNELLE DU RISQUE

Nous avons jusqu'à présent abordé trois aspects qui, d'après les propos recueillis auprès des interviewés, exercent une influence significative sur le processus décisionnel de gestion des risques informationnels. L'aspect contextuel constitue la première étape de l'élaboration d'un schéma tenant compte d'une approche multidimensionnelle du risque. En effet, il nous permet d'appréhender l'environnement de l'entreprise tel que le conçoit le gestionnaire de la sécurité, c'est-à-dire, en tenant compte d'une multitude de facteurs qui, selon lui, interviennent dans sa prise de décision relativement à la gestion des risques informationnels. L'aspect relationnel nous permet ensuite d'identifier un certain nombre d'acteurs qui, de par leur fonction, amènent le gestionnaire à se repositionner quant à sa participation dans le modèle de gouvernance de gestion des risques. Finalement, le profil du gestionnaire est le troisième et dernier aspect à s'imbriquer à cette structure. La richesse de son expérience, les connaissances dont il dispose et le poste qu'il occupe au sein de l'entreprise sont autant d'éléments qui nous renseignent sur la façon dont il aborde la gestion des risques informationnels.

[32] Sondages annuels de PricewaterhouseCoopers, Deloitte et Ernst & Young relativement aux risques informationnels (2010 à 2013).

Nous allons maintenant approfondir notre analyse en élaborant davantage sur la dynamique d'échange et de négociation entre les acteurs. Comme l'approche de la transaction sociale suppose «une vision complexe d'un acteur toujours situé, des forces qui le font agir (…) et de l'inextricable mélange des compétences dont il fait preuve» (Fusulier B. & N. Marquis 2008, p.20), il devient essentiel de révéler les dessous de la prise de décision du gestionnaire de la sécurité et de faire la lumière sur les règles écrites et non écrites que sous-tend ce processus.

L'analyse de la première partie de ce chapitre a démontré que la «sécurité de l'information», telle qu'on la concevait il y a quelques années, s'est progressivement départie de ses méthodes «extrémistes» pour adopter une approche plus terre-à-terre : «Maintenant, ça fonctionne pu être extrémiste. Faire peur pour essayer d'avoir plus de budget, ça fonctionne pu» (Interviewé 5). Non seulement la tentative d'influencer le sentiment d'insécurité demeure vaine mais il en résulte une augmentation de la vulnérabilité des systèmes d'information : les usagers se hasardent à contourner les politiques de sécurité en place et la direction autorise, de façon récurrente, des dérogations auxdites politiques. L'interviewé 11, fort de son expérience dans le domaine bancaire, relate les difficultés qu'il a lui-même rencontré dans ce milieu.

> «(…) Les banques sont forts pour les outils internes pis tout ça et ça revenait à chaque fois et à chaque fois, y avait des dérogations pis tout le monde le savait. Les dérogations sont revues à chaque année (…) et à chaque année, y étaient toujours réitérées et signées par le président».

Bien que cette problématique se rencontre encore fréquemment, les gestionnaires de la sécurité considèrent davantage le facteur «humain» dans l'équation sécuritaire. Qu'ils soient employés, cadres ou dirigeants, ce sont eux qui manipulent l'information. D'ailleurs, une majorité de gestionnaires nous ont confié que l'approche progressive[33] est maintenant celle qui doit être privilégiée : elle facilite l'intégration de nouvelles mesures de sécurité et cela, à tous les niveaux de l'entreprise, comme nous en a fait part

[33] Une approche progressive suppose une démarche étape par étape à moyen ou long terme.

ce gestionnaire : «(…) au-delà du profit pis de l'entreprise, c'est du monde…du monde qui se parle. Pis souvent le président, y veut juste être rassuré» (Interviewé 11). De fait, la gestion des risques informationnels passe désormais par la recherche d'un équilibre entre, d'une part, la mise en place d'outils et de politiques de sécurité adaptés au contexte organisationnel et, d'autres parts, les coûts engendrés par de tels outils. Comme le fait remarquer ce gestionnaire :

> «Ça demeure toujours une préoccupation pour nous de garder le bon balancier entre un accès simple, efficace et économique dans le cadre de nos opérations et la sécurité. Sans dire que c'est deux objectifs conflictuels, un vient empiéter sur l'autre. Il faut trouver la juste ligne. Si tu compenses avec une haute sécurité, tu deviens moins rapide donc moins compétitif et là bien, c'est toujours le jeu entre les deux» (Interviewé 10).

Ce que nous avons noté, c'est que tous les gestionnaires que nous avons rencontrés abordent la sécurité d'une façon qu'ils qualifient de «réaliste». On parle d'un retour à la base et aux principes simples qui en découlent. Ils existent, comme le souligne ce gestionnaire par exemple, «des contrôles souvent peu coûteux qui nous empêchent d'acheter des outils dispendieux et qui font la job pareil» (Interviewé 11). De plus, il est intéressant de constater que ce changement de mentalité dans la façon de gérer le risque informationnel coïncide avec la reconnaissance, par la direction, de la légitimité des dépenses en sécurité de l'information. En développant de nouveaux processus, en considérant les objectifs d'efficacité et de profitabilité de l'organisation et en proposant des solutions réalistes, les gestionnaires de la sécurité démontrent que leur implication au sein de l'organisation contribue à l'atteinte de ces mêmes objectifs. Bien qu'une majorité de gestionnaire dénotent encore une certaine réticence lorsqu'il est question de l'octroi de budget, cette réticence, faut-il le souligner, ne se limite pas uniquement au département de sécurité. Au contraire, la négociation de budget, comme la négociation de l'ajout de personnel, ou la négociation de contrat avec un fournisseur par exemple, constitue une part importante et même inévitable du travail du gestionnaire. Le fait que

le gestionnaire de la sécurité bénéficie en quelque sorte de ce «pouvoir» de négociation démontre qu'il a acquis un certain statut au sein de l'entreprise, un statut qui lui permet d'accomplir pleinement le mandat qui lui a été confié.

Néanmoins, les stratégies de négociation nécessitent un peu plus que des habiletés communicationnelles. Au moins la moitié des gestionnaires, provenant pour la plupart de grandes entreprises, nous ont confié que le processus de recommandation doit être savamment planifié et que sa présentation nécessite une argumentation alliant faits et prévisions à courts, moyens et longs termes. «(…) À ce jour, j'ai pas senti de difficultés à ce qu'on soit capable d'accomplir cette tâche-là et d'obtenir ce qu'il faut pour l'accomplir. Maintenant, c'est certain que nous, il faut qu'on aille de l'avant pour le proposer, c'est pas un réflexe» (Interviewé 14). Ce type d'échange entre la direction et les gestionnaires de la sécurité requiert par ailleurs, pour une meilleure collaboration et une confiance réciproque, le respect de certains principes de base comme la transparence, l'honnêteté et le leadership.

Ce sont ces mêmes principes qui contribueront à «créer de la rigueur dans toute la strate (…), au niveau opérationnel, au niveau politique et au niveau des processus» (Interviewé 9). Puisqu'une fois les recommandations acceptées, il reste à les mettre en place et à convaincre des dizaines, des centaines, voire même des milliers d'employés d'y adhérer. Six des quinze gestionnaires interviewés (Interviewés 2, 8, 9, 10, 13 et 15) nous ont fait remarquer que le leadership constitue un atout non-négligeable à cette étape du processus.

> «C'est pas les livres réglementaires qui vont faire que c'est plus «sécure» ou moins «sécure». En apparence possiblement : y a des lois, des règlements, y a des livres, des directives, des procédures…oui, mais ça reste un humain qui l'interprète et qui agit avec. (…) C'est le leadership, c'est l'attitude, c'est comment les dirigeants donnent l'exemple, appliquent la règle en bas que l'organisation marche ou ne marche pas» (Interviewé 10).

Pour cet autre gestionnaire, le principe est essentiellement le même : «Si tu fais ça, tu dis à tes 150 autres employés que c'est correct de faire ça» (Interviewé 9). Prêcher par l'exemple demeure, selon les gestionnaires interviewés, un moyen particulièrement efficace pour favoriser l'adoption de comportements sécuritaires lorsqu'il est question de risques informationnels. Rémy, dans sa présentation de la transaction sociale affirmait qu'il convient «de bien distinguer la situation dans laquelle le problème à résoudre se pose et le contexte» (Rémy 1996, p. 13). Un gestionnaire qui impose de nouvelles politiques de sécurité doit être conscient que les pouvoirs sont distribués inégalement et s'il veut atteindre son objectif et s'adjoindre une certaine collaboration des employés, il devra rééquilibrer les forces, ou du moins, donner cette impression qu'il est assujetti aux mêmes règles, aux mêmes politiques que tous les employés. Son comportement au quotidien, ses échanges avec les employés, témoigneront du compromis qu'il est prêt à faire et à s'imposer lui-même. Un atout qui lui permettra de négocier plus avantageusement l'adhésion aux politiques de sécurité.

Par ailleurs, la mise en place d'outils et de politiques de sécurité doit être adaptée au contexte et à la taille de l'organisation. Dans la petite entreprise, les gens se connaissent, se fréquentent et ont des contacts quasi quotidiens avec leur employeur et le gestionnaire de la sécurité. Ils sont conscients de leurs responsabilités mais aussi de celles des autres. La proximité rend la direction plus accessible et par conséquent, il devient plus aisé de communiquer l'information, d'identifier les problématiques et de trouver des solutions adéquates. «Étant une petite organisation, si on dit «maintenant la politique c'est ça» et si on l'explique clairement, les gens vont entrer dans le rang assez facilement» (Interviewé 3). Pour les plus grandes organisations, la mise en place de nouvelles procédures ou politiques de sécurité requiert une stratégie de communication et d'accompagnement complexe afin que tous les employés bénéficient de la même information et le cas échéant, d'une formation uniforme. Ce gestionnaire nous explique d'ailleurs que dès qu'un projet démarre, «la sécurité est tout de suite impliquée (…) J'ai mis en place toute une méthodologie d'accompagnement dans les projets» (Interviewé 5). Un autre gestionnaire (Interviewé 6) nous affirme avoir lui aussi mis en place une

procédure d'accompagnement lorsqu'il doit instaurer de nouvelles mesures de sécurité. Selon ce dernier, «avec un accompagnement, on s'assure d'une meilleure collaboration».

Ce que nous comprenons du discours de ces gestionnaires de la sécurité, c'est qu'ils doivent démontrer une implication constante, à tous les niveaux hiérarchiques et à toutes les étapes de la mise en place d'une politique ou d'un outil permettant à l'organisation de réduire les risques informationnels. Que ce soit à l'étape de la reconnaissance des risques jusqu'à l'accompagnement des employés dans l'adoption de comportements sécuritaires, le gestionnaire occupent à la fois trois rôles, indissociables : un rôle interpersonnel, un rôle informationnel et un rôle décisionnel (Schermerhorn, J. R. et al. 2010, p.19). Par conséquent, cela suppose que le gestionnaire de la sécurité appréhende le risque en tenant compte d'une multitude de facteurs contextuels, relationnels et individuels. Cela signifie également que même lorsqu'un gestionnaire privilégie l'analyse de risque par le biais d'une approche quantitative, il ne peut se soustraire à la composante qualitative, qui considère non seulement le profil et la personnalité du gestionnaire de la sécurité mais aussi la dynamique relationnelle à travers laquelle ce dernier s'engage. Et bien que le résultat de ses interactions avec les autres acteurs ne soit pas toujours appréciable, il n'en demeure pas moins réel et son influence sur le processus décisionnel de gestion des risques informationnels devient alors indéniable.

5.1 De la négociation à la transaction sociale

La négociation est d'ailleurs un élément particulièrement dominant au sein de cette dynamique relationnelle. Tel que l'ouvrage de Bourque et de Thuderoz (2011) le suggère, l'étude de la négociation relate principalement trois aspects: les dispositions des négociateurs, leur capacité de persuasion et leur expérience (à négocier face-à-face). Il s'agit, pour les gestionnaires qui vivent l'expérience de la négociation de convaincre sans imposer, d'accepter un compromis sans se soumettre mais surtout, de maintenir, voire même de renforcer les relations existantes et cela, même en situation de conflit

puisque soulignons-le, l'approche de la transaction sociale ne prétend pas que le conflit doit être évité à tout prix. Et comme nous l'ont mentionné plusieurs gestionnaires de la sécurité, le conflit, parfois inévitable dans un contexte où différentes constructions de la réalité et par extension, différentes constructions du risque s'affrontent, doit faire l'objet de discussions, de débats entre les acteurs concernés. Aussi, des intérêts qui semblent à prime à bord contradictoires se rejoignent parfois lorsqu'ils sont redéfinis à partir d'une perspective plus large qui considère la protection des actifs informationnels comme un objectif commun.

Il ressort également des propos des gestionnaires que dès qu'il est question d'identifier et de hiérarchiser un risque, il faut aussi prévoir ce que les différentes solutions envisagées impliqueront au niveau financiers, humains et technologiques. Du point de vue de la transaction sociale, le gestionnaire de la sécurité s'engagera donc dans une série d'interactions à différents niveaux et avec différents groupes, que ce soit avec les employés, la direction, les membres du comité de gouvernance ou une tierce partie, à l'interne ou à l'externe et cela à chaque étape du processus de gestion des risques informationnels. Ce que nous pouvons déduire de notre analyse, c'est que les gestionnaires qui s'engagent dans une analyse multidimensionnelle des risques informationnels (ce qui correspond à 86% de notre échantillon), considèrent non seulement les dimensions propres au contexte organisationnel mais ils sont également conscients des dynamiques relationnelles et des jeux de pouvoirs qui sont à l'œuvre au sein d'un tel processus. Leur propos suggèrent qu'ils en tiennent compte, tant dans leurs démarches de recommandations que dans les processus de négociation dans lesquels ils sont impliqués. Il semble que les gestionnaires ont su tirer avantage de cette prise de conscience en visant des objectifs de résultats et non de conflits et en acceptant, à l'occasion, de faire certains compromis.

Ils reconnaissent également que lorsqu'il est question de risques, personne ne détient le monopole de la vérité et personne ne sait exactement de quoi sera fait le futur. Le gestionnaire de la sécurité est ainsi confronté à une réalité qui se construit au fur et à mesure et qui n'est tangible que partiellement. Il doit pour ainsi dire accomplir ce qu'il

croit être optimal, compte tenu du contexte et du renseignement qu'il a su produire. Puisque la négociation porte, entre autres sur des faits passés et sur la possibilité qu'un ou plusieurs évènements se produisent, les résultats risquent de ne pas être ceux auxquels il s'attendait car l'acteur, au centre de ce processus, n'a de pouvoir que sur ses propres compétences techniques et relationnelles. La négociation ne consiste donc pas uniquement à s'appuyer sur une réalité existante mais également sur une réalité probable qui n'est définie qu'à travers un continuum de présomptions. C'est d'ailleurs pourquoi nous parlons d'un processus toujours en mouvement. Le processus décisionnel consiste en effet, pour le gestionnaire de la sécurité, à prendre position et à convaincre ses congénères et les membres de la direction que sa construction de la réalité, que sa vision des risques informationnels est assez réaliste pour entreprendre des actions concrètes qui visent soit la prévention d'un danger potentiel, soit la résolution d'un problème existant (dans un tel cas, le risque se serait alors matérialisé). Dans sa façon d'exprimer ce que représente la négociation, Eraly explique que «(…) ce n'est pas seulement les solutions qui sont négociées mais la définition même des problèmes» (Eraly 2008, p.80).

Quant au champ de la transaction sociale, plus large que celui de la négociation, il ne se limite pas qu'aux échanges verbaux mais s'étend aux «accords informels, implicites ou tacites» (Blanc 2009, p.128). Le mot négociation n'a pas à être prononcé, le conflit n'a pas à être manifeste. Lorsqu'un acteur occupe une position névralgique qui le situe au centre d'un processus décisionnel de gestion des risques, la dynamique relationnelle entre les intervenants suppose des échanges où «différentes logiques se confrontent» et où le conflit fait partie intégrante de ces échanges. Blanc souligne également que la gouvernance est elle-même considérée comme «un processus transactionnel entre de multiples acteurs, aboutissant à des compromis toujours provisoires, combinant les rapports de force et l'affectif» (Blanc 2009, p.133). Nous comprenons ainsi qu'il est tout à fait légitime de constater la présence de dissension entre les acteurs impliqués dans la gestion des risques informationnels. C'est dans la façon de négocier ces désaccords qu'il sera possible d'apprécier le rôle du responsable de la sécurité au sein de ce processus. Cet aspect de la transaction sociale nous renseigne également sur le champ élargi de

compétences que le gestionnaire doit posséder pour être en mesure de signifier efficacement son expertise.

Le processus décisionnel de gestion des risques informationnels dans lequel le gestionnaire de la sécurité s'engage implique aussi qu'il doit être sensible à d'autres formes d'interactions, à cette intuition qui lui permet de déceler les subtilités du comportement humain et qui peut faire de lui, ultimement, un meilleur stratège. La plupart des gestionnaires que nous avons rencontrés, forts de leur expérience, ont d'ailleurs fait allusion à ce «talent» particulier qu'ils ont su développé et qui leur permet d'exploiter leurs compétences relationnelles non seulement pour bâtir un renseignement de meilleure qualité mais également pour faire valoir leurs idées.

Nous pouvons finalement affirmer que la dimension relationnelle exerce une influence manifeste sur le processus décisionnel de gestion des risques informationnels. Cependant, les compétences techniques, l'expérience et la personnalité du gestionnaire demeurent des éléments essentiels qui sont pour ainsi dire, indissociables de la mise en place de solutions efficaces et efficientes qui sauront diminuer les risques de manière significative.

5.2 L'approche multidimensionnelle du risque

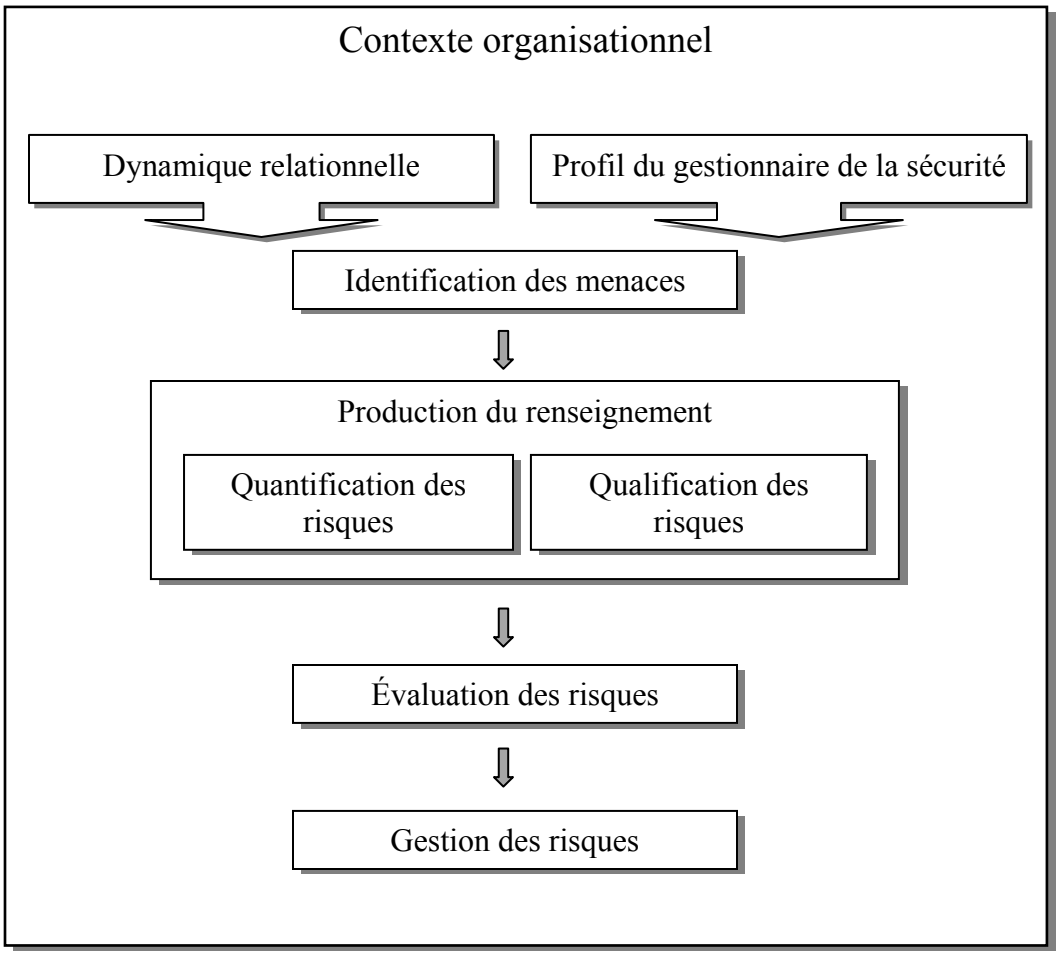
Nous nous devons par ailleurs d'apporter certaines explications complémentaires relativement à l'approche multidimensionnelle du risque car nous croyons qu'il s'agit d'un élément essentiel dont il faut tenir compte lorsqu'il est question de gestion des risques informationnels. D'abord, il faut comprendre qu'une multiplication des risques marquée par l'incertitude économique, politique, légale ou technologique pour ne nommer que celles-là suppose une gestion des risques informationnels marquée par l'accroissement des échanges entre acteurs, qu'ils se considèrent antagonistes, alliés ou les deux à la fois. Elle suppose aussi une analyse de risques qui tienne compte d'un

nombre incalculable de facteurs qui peuvent s'exprimer à travers deux composantes : une composante quantitative et une composante qualitative (constructiviste).

> «Opter pour une définition multidimensionnelle du risque présente l'avantage d'offrir un outil conceptuel riche, dans la mesure où 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, lesquelles figurent au programme d'une gestion des risques qui rende compte du pluralisme social et qui soit acceptable sur le plan de l'éthique» (Kermish 2012, p.6)

Dans plusieurs sphères d'activités, l'utilisation des méthodologies quantitatives pour opérationnaliser la gestion des risques est déjà bien établie et bien définie. Si Kermish prétend qu'il en va autrement pour la dimension qualitative ou constructiviste du risque, les entretiens effectués auprès des gestionnaires de la sécurité nous convainquent du contraire. En effet, nos données nous ont permis de constater que l'approche multidimensionnelle du risque constitue un mécanisme spontanément adopté par une majorité de gestionnaires. C'est-à-dire qu'en plus de s'intégrer naturellement au processus décisionnel de gestion des risques informationnels, la composante constructiviste du risque n'a pas à être définie. Elle se définit d'elle-même à travers les échanges auxquels le gestionnaire de la sécurité prend part et à travers le renseignement que ce dernier bâti au gré des informations qu'il reçoit, trie, analyse et structure. Si nous souhaitions donner une image à ce processus, il prendrait la forme suivante.

Figure 2. Gestion des risques informationnels[34]



Parce que la définition du risque est intrinsèquement subjective tant dans son approche quantitative que qualitative, elle se doit de considérer les «dimensions individuelles en interaction avec les dimensions collectives» (Kermish 2012, p.7). D'un point de vue pratique, nous avons pu constater qu'il est possible, voire même préférable pour les gestionnaires de la sécurité d'adopter cette approche, «ouverte et contextualisable» (Kermish 2012, p.12). Les gestionnaires que nous avons interviewés parlent d'une approche adaptative, réaliste, holistique. L'approche de la transaction sociale rend compte de cette dynamique et ne réduit pas le gestionnaire de la sécurité à un «acteur stratégique» : autrement dit, l'acteur et son environnement s'influence mutuellement ou

[34] Nous avons schématisé la gestion des risques informationnels en nous basant sur le processus élargi de gestion des risques élaboré par Kermisch en 2012.

de façon réciproque. Conséquemment, il s'exerce au sein du processus décisionnel une force qui n'est ni linéaire, ni constante, ni unidirectionnelle. Ce qui amène le gestionnaire, selon les propos que nous avons analysés, à s'adapter en fonction des enjeux et des facteurs contextuels internes et externes. Il doit également moduler son comportement, son attitude et son leadership en fonction de la pluralité des acteurs avec qui il transige. Pour ces raisons, l'approche de la transaction sociale et l'approche multidimensionnelle du risque sont indissociables dans la compréhension de la gestion des risques informationnels. Principalement, parce qu'elles rendent compte de toute la complexité du processus décisionnel sans qu'il soit nécessaire d'identifier un nombre prédéterminé de composantes ce qui, inévitablement nous conduirait à limiter notre perspective sociologique à quelques paramètres sans valeur puisque dépouillés de leur logique d'action.

Tout au long de cette recherche, les gestionnaires interrogés nous ont d'ailleurs confirmé que l'identification et la hiérarchisation des risques n'étaient réalisables qu'en tenant compte du contexte organisationnel et des mécanismes relationnels à l'œuvre au sein du processus de gestion des risques informationnels. Et bien que doté d'une volonté à toute épreuve, d'une solide expertise et de compétences relationnelles développées, le gestionnaire de la sécurité qui souhaite atteindre ses objectifs, ne pourra le faire qu'en ayant le support de la direction ou du comité de gouvernance le cas échéant. Nos données révèlent en effet que quatorze gestionnaires sur quinze privilégient une approche multidimensionnelle du risque mais que seulement la moitié l'applique concrètement. Résumons-le ainsi : nous avons certes amélioré notre compréhension de la gestion des risques informationnels en entreprise et la perspective des gestionnaires de la sécurité est autrement plus claire à ce sujet. Il n'en demeure pas moins que cette perspective, ce degré de conscientisation face à la protection du patrimoine informationnel se propage encore difficilement à travers les différentes strates de l'organisation (pour certaines d'entre elles il va s'en dire). Selon les gestionnaires de la sécurité, il s'agit là d'un travail colossal qui n'en est qu'à ses balbutiements.

6. CONCLUSION

6. CONCLUSION

Le rôle des gestionnaires de la sécurité s'est définitivement transformé au cours des dernières années et le développement des technologies de l'information n'y est pas tout à fait étranger. L'utilisation massive des médias sociaux de même que les vagues successives d'innovations des dispositifs de communication ont aussi contribué à l'évolution du concept même de «sécurité». Face à l'efficacité et à la rapidité de tels outils mais également face aux nouveaux risques que ces mêmes outils génèrent, les entreprises n'ont eu d'autres choix que de s'adapter. Le risque informationnel constitue désormais un enjeu majeur auquel l'entreprise ne peut se soustraire et sa gestion nécessite de nouvelles méthodes ainsi que l'élaboration d'un processus décisionnel qui tienne compte de la multiplication des vulnérabilités et de la complexité du contexte organisationnel. Jusqu'à présent, le rôle du gestionnaire de la sécurité au sein de ce processus demeurait flou et la définition de ses fonctions, longtemps associées à la protection des biens matériels souffrait de cette obsolescence. C'est à partir de ce constat que nous avons élaboré les objectifs de ce mémoire. Nous souhaitions comprendre, à partir de la perspective des responsables de la sécurité, comment s'effectue la gestion des risques informationnels et par l'entremise de quel processus ils identifient et hiérarchisent ces risques. Nous voulions aussi comprendre les mécanismes relationnels à l'œuvre et le rôle du responsable de la sécurité au sein de ce processus.

Nous pouvions d'ores et déjà nous demander si l'avènement de nouvelles menaces à la sécurité de l'information et leur médiatisation pouvaient à elles seules revendiquer la responsabilité d'un changement de mentalités de la part des dirigeants quant à l'utilité de la fonction «sécurité» dans l'entreprise. Nous nous sommes aussi demandé si ce changement provenait d'un décloisonnement des fonctions de l'entreprise, reléguant du même coup la sécurité à la prévention des pertes, au contrôle d'accès et à la surveillance par caméras. Ce qui, par conséquent, aurait pu laisser croire que la gestion des risques informationnels pouvait relever d'un autre

département ou même pouvait devenir l'objet d'un contrat exécuté par une firme externe.

Nos premières tentatives pour recruter des participants nous ont cependant aiguillées vers une piste à laquelle nous n'avions pas songé. S'il y a effectivement un décloisonnement des fonctions de l'entreprise, l'objectif est avant tout de favoriser le processus de gouvernance de la sécurité de l'information et de promouvoir la communication entre les intervenants. Dans cette optique, l'aspect relationnel de la gestion des risques prend une toute autre signification puisqu'il s'étend bien au-delà de l'organisation; des firmes conseils aux intervenants étatiques en passant par les compétiteurs, aucune source n'est négligée lorsqu'il est question de détecter les vulnérabilités et de protéger les actifs de l'entreprise.

Bien que dans le commerce de détail, la prévention des pertes demeure la principale responsabilité du gestionnaire de la sécurité, il n'en demeure pas moins que cette responsabilité s'imbrique dans un processus de gestion beaucoup plus complexe qui tient compte d'une multitude d'éléments que nous avons nommé le contexte organisationnel. Ce deuxième aspect s'est révélé plus complexe à traiter dans la mesure où l'identification desdits éléments (innombrables faut-il le dire) relève d'un exercice qui dépasse le cadre de ce travail. C'est pourquoi nous nous sommes concentrés sur les catégories qui nous semblaient les plus pertinentes et sur lesquelles les gestionnaires avaient davantage élaborés. Parmi celles-ci, notons la multiplication des enjeux sécuritaires liés principalement à l'utilisation des nouvelles technologies, la complexité du cadre réglementaire surtout lorsque celui-ci s'étend au-delà des frontières canadiennes, les contraintes budgétaires et un nombre non négligeable de problématiques créées par une utilisation inadéquate ou abusive des systèmes d'information. Nous avons par ailleurs constaté que la fonction «sécurité» s'est progressivement intégrée à la structure décisionnelle de l'entreprise par un enrichissement des tâches, un élargissement des responsabilités mais aussi par une reconnaissance des compétences et du leadership dont font preuve les quinze gestionnaires de la sécurité que nous avons rencontré. Ces derniers témoignent tous

d'une riche expérience dans leur domaine d'expertise respectif et démontrent, pour la plupart d'entres eux, une volonté de parfaire leur éducation et d'améliorer leurs connaissances. Non seulement doivent-ils être au fait des dernières tendances de l'industrie en matière de protection des actifs mais ils doivent également détenir certaines compétences clés leur permettant d'instaurer mesures et politiques de sécurité tout en s'assurant la collaboration des employés, des cadres et des membres de la direction.

Lors de nos entrevues, nous nous sommes ainsi rendu compte que la responsabilité des gestionnaires de la sécurité en matière de gestion des risques informationnels requiert l'assimilation de concepts liés au comportement organisationnel, des habiletés communicationnelles développées et des aptitudes de stratège. L'implication de plusieurs acteurs au sein du processus décisionnel de gestion des risques informationnels suppose également des jeux de pouvoir et de négociation. Toutefois, l'efficacité de la négociation repose sur une stratégie de résolution de problème qui vise la formulation de solutions acceptables pour toutes les parties et où les objectifs respectifs peuvent être atteints (objectifs sécuritaires et objectifs de profitabilité de l'organisation). L'homogénéité dans le discours des gestionnaires nous a par ailleurs surpris puisque même si les études de grandes envergures nous permettaient d'envisager la possibilité que de plus en plus de gestionnaires optent pour des solutions réalistes adaptées au contexte de l'entreprise, nous ne pouvions imaginer que la totalité des participants partageraient cet avis. Et bien qu'il soit difficile de généraliser les résultats de notre recherche à l'ensemble des gestionnaires de la sécurité qui exercent des fonctions similaires, les résultats de notre analyse nous permettent d'envisager une tendance vers laquelle ces derniers solidifieraient leur apport au modèle de gouvernance de la sécurité de l'information dans l'entreprise.

Le rôle du gestionnaire de la sécurité en matière de gestion des risques informationnels est encore appelé à se transformer et l'évolution de sa sphère d'activités n'aura de limite que ses compétences, son expertise, ses aptitudes relationnelles de même que sa capacité à fournir des réponses «adaptée aux enjeux»

auxquels son organisation sera confrontée (Livre Blanc du CDSE). Notre façon d'aborder la gestion des risques informationnels, peu importe qu'il s'agisse d'organisations publiques ou privées devra refléter cette complexité et surtout, notre analyse aura tout intérêt à ne négliger aucune dimension, qu'elle soit quantitative ou qualitative, sachant que le contexte organisationnel et les interactions sociales jouent un rôle déterminant à toutes les étapes du processus décisionnel.

Bibliographie

- Alexandre-Leclair, L. (2001). *Les pratiques du portage commercial à l'international, le rôle des stratégies de contre-intelligence économique et stratégique*. Thèse en Sciences de Gestion soutenue le 18 décembre 2001, IAE de Lyon-Université Jean Moulin Lyon 3.

- Allaire, Y. (2012). *Les prises de contrôle de sociétés québécoises : enjeux et pistes de solution*. Institut pour la gouvernance d'organisations publiques et privées IGOPP.

- Ashenden, D. (2008). Information security management: a human challenge? *Information Security Technical Report*, vol. 13, pp. 195-201.

- Bahri, S. & H. Hadj Mabrouk (2009). *L'Intégration de la Sécurité dans les Systèmes Technologiques de l'Information et de la Communication*. SETIT 2009 5th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications. March 22-26, 2009 – TUNISIA.

- Baumard, P. (2002). «Les paradoxes de la connaissance organisationnelle» dans Josserand & Perret, *Les paradoxes de la connaissance*, Paris : Ellipses.

- Beck U. (1986). *Risk Society: Towards a New Modernity*. London: Sage.

- Beck U. (2001). *La société du risque. Sur la voie d'une autre modernité*. Paris : Éditions Aubier.

- Berg, J. & C. Shearing (2008). Integrated Security: Assembling Knowledge's and Capacities. Dans *The Handbook of Knowledge Based Policing: Current Conceptions and Future Directions*. Editor: Tom Williamson.

- Berger, P. L. & Luckmann, Th. (1986). *La construction sociale de la réalité*. Paris : Méridiens-Klincksieck.

- Beldjilali, T. (2009). La sécurité des systèmes d'information en entreprise. *Communications of IBIMA*, vol. 9, pp. 156-162.

- Blanc, M. (2009). L'avenir de la sociologie de la transaction sociale. *Recherches sociologiques et anthropologiques.* vol.40 no. 2, pp.125-139.
  Consulté le 03 novembre 2012.
  URL : http://rsa.revues.org/157; DOI : 10.4000/rsa.157

- Bourque, R & C. Thuderoz (2011). *Sociologie de la négociation*, Nouvelle édition, avec études de cas. Rennes, PU Rennes : Collection Didact Sociologie.

- Brodeur, J.-P. (2007). High and Low Policing in Post-9/11 Times. *Policing, Oxford Journal*, Vol. 1, no. 1, pp. 25-37.

- Brodeur, J.-P. and Dupont, B. (2008). Introductory Essay: The Role of Knowledge and Networks in Policing. Dans: *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions*, Editor: Tom Williamson, pp. 9-34.

- Bulinge, F. (2002). *Pour une culture de l'information dans les petites et moyennes organisations : un modèle incrémental d'intelligence économique*. Université de Toulon et du Var, laboratoire Lepont. (Thèse)

- Button, M. (2008). *Doing security: Critical reflections and an agenda for change*. Palgrave Macmillan.

- Coskun Samli, A. & L. Jacobs (2003). Counteracting Global Industrial Espionage: A Damage Control Strategy. *Business and Society Review*, vol. 108, no. 1, pp. 95-113.

- Cox, J (2009). *Le renseignement: définitions, notions et gouvernance*. Division des affaires sociales. Parlement du Canada.
  http://www.parl.gc.ca/content/lop/researchpublications/prb0922-f.htm
  Consulté le 12 octobre 2012.

- Crozier, M. & E. Friedberg (1981). *L'acteur et le système : les contraintes de l'action collective.* Édition du Seuil.

- Culet A. & F. Bounass (1994). Développement d'une base de connaissances pour le bâtiment. *Représentations par objets, Actes des journées* EC2, RPO, Paris.

- Danielson, M. (2009). Economic Espionage: A framework for a workable solution. *Minnesota Journal of Law, Science and Technology*, vol. 10, no.2, pp. 503-548.

- Davenport, T. H. (1997). *Information Ecology*. Oxford University Press.

- Davenport, T. H. & L. Prusak (1998). *Working knowledge: How organisations manage what they know*. Harvard Business press.

- Delbecque, E. (2008). *Protection et défense du patrimoine informationnel et des connaissances.* 4ème pôle OCDIE.
  URL www.intelligence-economique.gouv.fr/IMG/pdf/**ocdie**_4.pdf

- Denis, J. (2009). Sécurité informatique et valeur des écrits au travail. *Revue de sémiolinguistiques des textes et discours*. Vol.28, pp. 85-100
  Consulté le 20 octobre 2012
  URL : http://semen.revues.org/8732

- Denzin N. K. & Lincoln Y. S. (1994). *Handbook of qualitative research*. Thousand. Hope, CA : Sage.

- Deslauriers, J.-P. & M. Kérisit (1997). Le devis de recherche qualitative. Dans Poupart et al. *La recherche qualitative: enjeux épistémologiques et méthodologiques*. Boucherville: Gaétan Morin.

- Dionne, G. (2013). *Gestion des risques: histoire, définitions et critiques*. http://neumann.hec.ca/gestiondesrisques/13-01.pdf

- Douglas, M. & A. Wildavski (1983). *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. University of California Press.

- Dupont, B (2006). Delivering security through networks: Surveying the relational landscape of security managers in an urban setting. *Crime, Law and Social Change*, vol. 45, pp.165-184 : Springer.

- Dupont, B. (2006). La sécurité intérieure au XXIe siècle : l'émergence des réseaux.In P. Zen-Ruffinen (sous la direction de), *Mélanges dédiés au professeur Bolle,* Helbing & Lichtenhahn, Neuchâtel, 2006, pp. 347-358.

- Dupont, B. (2010). Les organisations : sentinelles aveugles de la sécurité des données personnelles. *Sécurité & Stratégie*, no. 3.

- Ebondo Wa Mandzila, E. & D. Zéghal (2009). Management des risques de l'entreprise : ne prenez pas le risque de ne pas le faire. *La Revue des Sciences de la Gestion*, vol. 3, no. 237-238, pp. 5-14.

- Eraly A. (2008). Les limites de la négociation : penser la négociation. De Boeck Supérieur : *Ouvertures sociologiques*, pp. 77-82.

- Ericson, R. & M. Leslie (2008). The architecture of risk management. *Economy and society,* vol. 37, no. 4, pp. 613-624.

- Erickson, V. et K. D. Haggerty (1997). *Policing the risk society*. Oxford University Press.

- Faucon B. & S. Gaultier-Gaillard (2010). Les enjeux de sûreté dans un environnement concurrentiel : un défi pour les entreprises. *Sécurité et Stratégie*, no.3, mars 2010, pp.49-57

- Fenneteau, H. (2002). *Enquête: entretien et questionnaire*. Paris : Dunod.

- Fisher, R.J., E. Halibozek & G. Green (2008). *Introduction to security*. Eighth Edition, Butterworth-Heinemann, Elsevier.

- Foryst, C. A. (2010). Rethinking National Security Strategy Priorities, *International Journal of Intelligence and Counterintelligence,* Vol. 23, no. 3, pp. 399-425.

- Foucart et al. (2013). Penser et agir dans l'incertain : l'actualité de la transaction sociale. Éditorial. De Boeck Supérieur. *Pensées Plurielle*, vol. 2-3, no. 33-34, pp. 7-19.

- Foudriat, M. (2010). *Sociologie des organisations*, 3e éditions : Pearson.

- Fusulier B. & N**.** Marquis (2008). La notion de transaction sociale à l'épreuve du temps. *Recherches sociologiques et anthropologiques*, vol. 39, no. 2, pp.3-21,

- Fusulier, B. & et N**.** Marquis (2009). Faire une sociologie de la transaction sociale ou de la transaction sociale une sociologie? *Recherches sociologiques et anthropologiques*, vol. 40, no. 2, pp. 141-147.

- Ghernaouti-Hélie, S. (2007). Cybercriminalité et sécurité intérieure : état des lieux et éléments de prévention. Dans Cusson, Dupont et Lemieux, *Traité de sécurité intérieure* (2007). Cahiers du Québec, Collection Droit et Criminologie, Éditions HMH.

- Ghiglione R. & B. Matalone (1978). *Les enquêtes sociologiques. Théories et pratiques*. Paris: Armand Colin.

- Gibout C. & I. Zwarterook (2013). Gérer les risques industriels et la pollution dans le Dunkerquois : une double échelle transactionnelle. De Boeck Supérieur, *Pensée Plurielle* vol. 2-3, no. 33-34 pp. 131-148. http://halshs.archives-ouvertes.fr/halshs-00984745

- Gilbert C. (2003). La fabrique des risques. *Cahiers internationaux de sociologie,* vol. 1, no. 114, pp. 55-72.

- Harbulot, C., D. Lucas et N. Moinet (2002). *La guerre cognitive : vers la recherche de la suprématie stratégique.* XI^{ième} Colloque International de l'Association Aéronautique et Astronautique de France.

- Hassid, O. (2008). *La gestion des risques*, 2^{e} Édition. Collection Les Topos: Dunod.

- Johnston, L. & C. D. Shearing (2003). *Governing security: exploration in policing and justice*. Routledge.

- Kaplan, S. & B. John Garrick (1981). On the quantitative definition of risk. *Risk Analysis*, vol.1, no.1, pp. 11-18

- Kermisch, C. (2012). Vers une définition multidimensionnelle du risque. *VertigO - la revue électronique en sciences de l'environnement.* Vol. 12, no. 2.
  Consulté le 13 novembre 2012
  URL http://vertigo.revues.org/12214 ; DOI : 10.4000/vertigo.12214

- Klinke, A. & O. Renn (2002). A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies. *Risk Analysis,* vol. 22, no. 6, pp. 1071-1094.

- Kwak, Y. H. & K. S. Laplace (2005). Examining risk tolerance in project-driven organization. *Technovation*, vol. 25, pp. 691-695.

- Lagadec, P. (1981). *Le risque technologique majeur : politique, risque et processus de développement*. Paris, Pergamon Press.

- Lajili K. & Zégal D. (2005). Gérer le risque à l'échelle de l'entreprise : l'autre facette de la gouvernance d'entreprise. *Revue Gestion*, vol. 30, pp. 104-114.

- Laperrière, A. (1997). Les critères de scientificité des méthodes qualitatives. Dans Poupart et al. *La recherche qualitative: enjeux épistémologiques et méthodologiques*. Boucherville: Gaétan Morin.

- Larivet, S. (2009). *Intelligence économique : enquête dans 100 PME*. L'Harmattan.

- Le Blanc et al. (2013). La concertation sur les risques industriels : 10 pistes d'amélioration. *Cahiers de la sécurité industrielle*. No. 2013-09. Fondation pour une culture de sécurité industrielle, Toulouse, France. (ISSN2100-3874)
  http://www.foncsi.org/.

- Léger, M-A (2004). *Méthodologie de gestion du risque en matière de sécurité de l'information*. Éditions Fortier : Communications, Bibliothèque nationale du Québec.

- Léger, M.-A. (2008). Sommaire des résultats et points culminants de l'audit de sécurité sans fil réalisé à l'hiver 2008 sur la Rive-Sud de Montréal (Québec), http://www.leger.ca/pages/CHAMPLAIN/audit_wifi.htm

- Leman-Langlois, S (2007). L'analyse de problème de sécurité et la conception de solutions adaptées. Dans Cusson, Dupont et Lemieux, *Traité de sécurité intérieure,* Collections du Québec : Collection Droit et Criminologie, pp.199-221.

- Lessard, B. (2009). *Cadre de la gestion de la sécurité de l'information*. Bureau de la sécurité de l'information. Ressources naturelles et faune Québec. Gouvernement du Québec.

- Lévy, A. (1974). L'interprétation des discours. *Connexions,* no 2, pp. 43-63.

- March, J. G. & Z. Shapira (1987). Managerial perspectives on risk and risk-taking. *Management Science*, vol. 33, no. 11, pp. 1404-1418.

- Maroy, C. (2009). La transaction sociale en débat, *Recherches sociologiques et anthropologiques*. Vol. 40, no. 2. pp.121-123.
  Consulté le 15 mars 2013
  URL : http://rsa.revues.org/155

- Mary, P. (2005). Les figures du risque et de l'insécurité. *Informations sociales* vol. 6, no. 126, p. 16-25.

- McFadzean, E., J.-N. Ezingeard, & D. Birchall (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review*, vol. 31, no.5, pp. 622-660.
  Consulté le 04 novembre 2012.
  http://dx.doi.org/10.1108/14684520710832333

- Mignault, S. (2007). L'audit de sécurité et la protection des organisations. Dans Cusson, Dupont et Lemieux : *Traité de sécurité intérieure*. Collections du Québec : Collection Droit et Criminologie, pp. 387-399.

- Miles, M. B. (1979). Qualitative Data as an Attractive Nuisance: The Problem of Analysis. *Administrative Science Quarterly*, vol. 24, no. 4, pp. 590-601.

- Morizot, H. (2011). *L'intelligence des risques», Introduction à l'intelligence économique et à la protection du patrimoine informationnel.* École Européenne d'intelligence économique.

- Morse, J. M. (1994). Designing funded qualitative research. Dans N. K. Denzin & Y. S. Lincoln (eds.), *Handbook of Qualitative Research*. Thousand Oaks, CA. Sage, pp. 220–235.

- Mulone, M. & C. Desroches (2012). Que savons-nous de la consommation de la sécurité? *Revue Internationale de Criminologie et de Police Technique et Scientifique*, Volume LXV(3), 283-304.

- Muramatsu, K. (2013). La transaction comme forme de la politique et de la société face au risque. De Boeck Supérieur, *Pensée Plurielle* vol. 2-3, no. 33-34 pp. 149-162. http://halshs.archives-ouvertes.fr/halshs-00984745

- Nasheri, H. (2005). Economic Espionage and Industrial Spying, *Cambridge Studies in Criminology*. Kent State University, Ohio.

- Nécol, Charles. (2005). *La prévention spécialisée et la lutte contre l'insécurité*. IRTS de Lorraine, Metz. (Mémoire)

- Nonaka, I. (1994). A dynamic theory of organizational knowledge creation, *Organization Science*, vol.5, no.1, pp.14-37.

- Ocqueteau, F. (2011). Profils et trajectoires des directeurs sûreté. Résultat d'une enquête conduite auprès de 25 entreprises. *Sécurité & Stratégie*, vol. 5, pp. 38-53.

- O'reilly, C., & G. Ellison (2006). Eye Spy Private High: Re-Conceptualizing High Policing Theory. *The British Journal of Criminology*, vol. 46, no. 4, pp. 641-660.

- Paille, P. & A. Mucchielli (2005). *L'analyse qualitative en sciences humaines et sociales,* Paris : Armand Collin.

- Patton, M. (1990). *Qualitative evaluation and research methods* 2nd Edition. Newbury Park, CA. Sage

- Pires, A.P. (1997). Échantillonnage et recherche qualitative : essai théorique et méthodologique. Dans Poupart et al. *La recherche qualitative: enjeux épistémologiques et méthodologiques*. Boucherville: Gaétan Morin.

- Posthumus S. & R. von Solms (2004). A framework for the governance of information security. *Computers & Security* , vol. 23, pp. 638-646.

- Poupart, J. & al. (1997). *La recherche qualitative: enjeux épistémologiques et méthodologiques*, Boucherville: Gaétan Morin.

- Quivy, R. & L. Van Campenhoudt (1988). *Manuel de recherche en sciences sociales*. Paris : Dunod.

- Renn O. (1992) *Concept of risk: a classification*. Chapitre 3, pp. 53-79. Document PDF elib.uni-stuttgart.de

- Rhee, H.-S., Ryu, Y-U. & C.-T. Kim (2012). Unrealistic optimism on information security management. *Computer and Security*, vol. 31, pp. 221-232.

- Rémy J. (2005). Négociations et transaction sociale. *Négociations*, vol.1 no. 3, pp. 81-95.

- Rémy, J. (1996). La transaction, une méthode d'analyse : contribution à l'émergence d'un nouveau paradigme. *Environnement et Société*, no. 17, pp. 9-31.

- Rémy, J., Voyé, L. & E. Servais (1978). *Produire ou reproduire. Une sociologie de la vie quotidienne*. Bruxelles, Vie Ouvrière.

- Roper, C. A (1999). *Risk management for security professionals*. Butterworth-Heinemann.

- Rudman, R.J. (2010). Incremental risks in Web 2.0 applications. *The Electronic Library*, vol. 28 no. 2, pp. 210-230.

- Santoni, J.-L. (2006). *Qualification et quantification des risques en vue de leur transfert : la notion de patrimoine informationnel*. Actes du symposium SSTIC06

- Schermerhorn, J. R. et al. (2010). *Comportement humain et organisation*, 4e édition : Édition du renouveau pédagogique Inc.

- Shedden, P. & al. (2012). Incorporating a knowledge perspective into security risk assessments. *VINE*, vol.41, no. 2, pp. 152-166.

- Silverman, D. (2005). *Doing Qualitative Research*, Second Edition. London: Sage.

- Slovic, P. et E. U. Weber (2002). Perception of Risk Posed by Extreme Events. Conference: *Risk Management strategies in an Uncertain World*, Palisades, New York, April 12-13, 2002.

- Steinbart & al. (2012). The relationship between internal audit and information security: an exploratory investigation. *International Journal of Accounting Information Systems*, vol. 13, pp. 228-243.

- Tsoumas, V. & T. Tryfonas (2004). From risk analysis to effective security management: towards an automated approach. *Information Management & Computer Security,* vol. 12, no. 1, pp. 91-101.

- Thuderoz, C. (2010). *Sociologie des entreprises*, 3e éditions. Éditions La Découverte.

- Van Maanen, J. (1983). *Qualitative Methodology*. London : Sage

- Von Solm, B. (2001). Corporate governance and information security. *Computers and security*, vol. 20, pp. 215-218.

- Vuillerme, J.-P. (2010). Vers une vision extensive de la protection de notre patrimoine industriel, scientifique et technologique. *Sécurité et Stratégie*, vol. 3, pp. 62-73.

- Wildavsky, A. et K. Dake (1990). Theories of risk perception: Who fear what and why? *Daedalus,* Vol. 119, No. 4, pp. 41-60. The MIT Press on behalf of American Academy of Arts & Scienceshttp://www.jstor.org/stable/20025337

- Williamson, T. (2008). *The Handbook of knowledge based policing: Current conceptions and future directions*. John Wiley & Sons.

- Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization*, vol.16, Issue 4, 2006, 304-324

- Whitman, M. E. & H. J. Mattord (2005). *Principles of Information Security,* 2nd ed. Course Technology. Boston, MA

- Wood, J. & B. Dupont (2006). *Democracy, society and governance of security*. Cambridge University Press.

- Yildirim, E. Y. & al. (2011). Factors influencing information security management in small and medium sized enterprises: a case study from Turkey. *International Journal of Information Management*, vol.31, pp. 360-365.

- Zwaterook, I. (2013). Gérer les risques industriels et la pollution dans le Dunkerquois : une double échelle transactionnelle. *Pensée plurielle*, vol.2-3, no. 33-34, pp. 131-148.

- (auteur non identifié) (2000). The Corporate Security Officers: Understanding What They Do and Are They Doing Their InfoSec Part? *Computer Fraud and Security***,** vol. 2000, Issue 11, p. 18-20.

Rapports de l'industrie, publications gouvernementales et conférences

- Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence (document prepared by Dennis C. Blair, Director of National Intelligence) February 2, 2010.

- Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY 2008. Office of National Counter Intelligence Executive, Washington, DC. Report on July 2009.

- Breaking barriers. 2012 DTTL Global Financial Services Industry Security Study. Deloitte (2012)

- Blurring the lines. 2013 TMT Global Security Study. Deloitte (2013).

- CDSE. Livre Blanc. La fonction sûreté dans l'entreprise: Quelles réponses à quelles problématiques? Club des Directeurs de Sécurité des Entreprises (CDSE), Paris, Décembre 2011.

- CDSE. Commission IE 2010.

- CIGREF 2007. Protection du patrimoine informationnel.

- CIRANO. Lettre CIRANO – Centre interuniversitaire de recherche en analyse des organisations. Le risque au CIRANO. Mai 2005.

- COSO 2005. Le management des risques de l'entreprise – Cadre de référence.

- Federal Information Security Management Act (FISMA). 2004 Report to Congress. Office of Management and Budget, USA.

- Fighting to close the gap, Global Information Security Survey. Ernst & Young's (2012).

- FIPS PUB 199. Standards for security categorization of Federal Information and information systems. Computer Security Division. National institute of standards technology, Gaithersburg, MD. 20899-8900.

- Into the cloud, out of the fog, Global Information Security Survey. Ernst & Young's (2011).

- Le Livre Bleu. Développer la culture des risques informatiques et informationnels. Réalisé par HAPSIS pour les Assises de la sécurité et des systèmes d'information, Octobre 2009.

- Panorama 2008-2009 des crimes commis contre les entreprises, Enquêtes EDHEC-CDSE. Sécurité et Stratégie, no.3, mars 2010, pp.7-13.

- Protecting what matters. The 6th Annual Global Security Survey. Deloitte (2009)

- Raising the Bar. 2011 TMT Global Security Study. Deloitte (2011)

- SANS Institute. Information security: starting out. SANS Institute Information security reading room (2009).
- The faceless threat. Financial Services Global Security Study. Deloitte (2010)
- Trial by fire. PricewaterhouseCoopers (2009).
- The Global State of Information Security Survey. PricewaterhouseCoopers (2010).
- The Global State of Information Security Survey. PricewaterhouseCoopers (2011).
- The Global State of Information Security Survey. PricewaterhouseCoopers (2012).
- The Global State of Information Security Survey. PricewaterhouseCoopers (2013).
- Trends in Proprietary Information Loss. Survey Report. ASIS International (2007).
- Under cyber-attack, Global Information Security Survey. Ernst & Young's (2013).
- Verizon. 2014 Date breach investigations report.
- 2014 Information security Breaches survey. Department for business, innovation and skills. United Kingdom.

ANNEXE A

CARACTÉRISTIQUES DE L'ÉCHANTILLON

Sujet	Fonction	Expérience	Taille de l'entreprise[35]	Industrie	Risque global[36]
S1	Gestionnaire T/I	Civile	Grande	Transport	Élevé
S2	Gestionnaire sécurité	Militaire	Grande	Transport	Élevé
S3	Gestionnaire T/I	Civile	Petite	Sécurité	Faible
S4	Gestionnaire sécurité	Civile	Petite	Sécurité	Faible
S5	Gestionnaire T/I	Civile	Grande	Commerce de détail	Faible
S6	Gestionnaire sécurité	Civile	Grande	Logiciel	Moyen
S7	Gestionnaire T/I	Civile	Petite	Logiciel	Moyen
S8	Gestionnaire sécurité globale	Militaire	Grande	Ressources naturelles	Élevé
S9	Gestionnaire sécurité	Civile	Moyenne	Commerce de détail/ services	Faible
S10	Gestionnaire sécurité	Police	Grande	Sécurité	Moyen
S11	Gestionnaire T/I	Civile	Grande	Média	Faible
S12	Gestionnaire sécurité	Police	Grande	Commerce de détail	Faible
S13	Gestionnaire sécurité	Civile	Grande	Commerce de détail	Faible
S14	Gestionnaire T/I	Civile	Grande	Commerce de détail	Faible
S15	Gestionnaire sécurité	Civile	Grande	Commerce de détail	Faible

[35] Structure selon le nombre d'effectifs. Petites entreprises : moins de 100 employés. Moyennes entreprises : entre 100 et 499 employés. Grandes entreprises : plus de 500 employés. Source : *Industrie Canada*. http://www.ic.gc.ca/eic/site/061.nsf/fra/02719.html

[36] Évaluer d'après le cadre de référence COSO 2 (Committee Of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management Framework), le FIPS (Federal information processing standards publication) et Panorama 2008-2009 des crimes commis contre les entreprises. Enquêtes EDHEC-CDSE *Sécurité et Stratégie*, no.3, mars 2010, pp.7-13

#

ANNEXE B

SCOLARITÉ ET APPARTENANCE À UN RÉSEAU

Sujet	Fonction	Scolarité	Membre d'un réseau professionnel	Membre d'un comité ou d'un conseil de direction
S1	Gestionnaire T/I	Universitaire 1er cycle	Oui	Oui
S2	Gestionnaire sécurité	Universitaire 2e cycle	Oui	Oui
S3	Gestionnaire T/I	Universitaire 2e cycle	Oui	Oui
S4	Gestionnaire sécurité	Collégiale	Oui	Oui
S5	Gestionnaire T/I	Universitaire 1e cycle	Oui	Oui
S6	Gestionnaire sécurité	Universitaire 1er cycle	Oui	Oui
S7	Gestionnaire T/I	Universitaire 1er cycle	Oui	Oui
S8	Gestionnaire sécurité globale	Collégiale	Oui	Oui
S9	Gestionnaire sécurité	Collégiale	Oui	Oui
S10	Gestionnaire sécurité	Universitaire 1er cycle	Oui	Oui
S11	Gestionnaire T/I	Collégiale	Non	Non
S12	Gestionnaire sécurité	Universitaire 1er cycle	Oui	Oui
S13	Gestionnaire sécurité	Collégial	Oui	Non
S14	Gestionnaire T/I	Universitaire 1er cycle	Non	Oui
S15	Gestionnaire sécurité	Universitaire 1er cycle	Oui	Non

ANNEXE C

THÈMES ET CATÉGORIES

1. ASPECTS CONTEXTUELS
    a. ENJEUX
        I. VOL ET PERTE DE DONNÉES MATÉRIELLES
        II. VOL DE DONNÉES VIA LES TRANSACTIONS P.O.S. (commerce au détail)
        III. PIRATAGE INFORMATIQUE
        IV. NÉGLIGENCE DES EMPLOYÉS
        V. MALVEILLANCE DES EMPLOYÉS
        VI. ESPIONNAGE INDUSTRIEL
        VII. PRISE DE CONTRÔLE HOSTILE
        VIII. ATTEINTE À LA RÉPUTATION DE L'ENTREPRISE
        IX. DIFFICULTÉ À IDENTIFIER LES ACTIFS INFORMATIONNELS
        X. PROTECTION DU SAVOIR-FAIRE, DE L'INTÉGRITÉ DES PROCESSUS
        XI. NOUVELLES TECHNOLOGIES

    b. CONTRAINTES
        I. NORMES ET STANDARDS
        II. LOIS ET RÈGLEMENTS
        III. RESTRUCTURATION EN FONCTION DES NIVEAUX DE SÉCURITÉ
        IV. LOURDEUR DU PROCESSUS DÉCISIONNEL
        V. BUDGET
        VI. CONTRAINTES HUMAINES

    c. OPPORTUNITÉS
        I. NOUVELLES TECHNOLOGIES
        II. LOIS ET RÈGLEMENT
        III. NORMES ET STANDARDS

    d. TOLÉRANCE AU RISQUE
        I. STADE DE DÉVELOPPEMENT DE L'ORGANISATION
        II. PERSONNALITÉ DES DIRIGEANTS
        III. STRUCTURE DE L'ORGANISATION
        IV. TOLÉRANCE AU RISQUE DES TIERCES PARTIES
        V. CULTURE INFORMATIONNELLE
        VI. SITUATION FINANCIÈRE DE L'ORGANISATION

2. ASPECT RELATIONNEL
    a. INTERNE
        I. DIRECTION/EXÉCUTIF
        II. CHEF DE DIVISION
        III. INTERDÉPARTEMENTAL (JURIDIQUE, FINANCE, MARKETING, RESSSOURCES HUMAINES, OPÉRATIONS, ADMINISTRATIF)
        IV. EMPLOYÉS

V. COLLÈGUES
VI. VÉRIFICATEURS
VII. SYNDICAT
VIII. COMITÉ DE GOUVERNANCE
IX. COMITÉ DE DIRECTION
X. SÉCURITÉ TI (DANS LE CAS D'UN GESTIONNAIRE DE LA SÉCURITÉ PHYSIQUE)
XI. SÉCURITÉ PHYSIQUE (DANS LE CAS D'UN GESTIONNAIRE DE LA SÉCURITÉ TI

b. EXTERNE
I. AUTORITÉS PUBLIQUES
II. GOUVERNEMENT ET MUNICIPALITÉS
III. SERVICES SECRETS LOCAL OU ÉTRANGER
IV. FIRMES DE VÉRIFICATEURS
V. ORGANISMES DE CERTIFICATION
VI. FIRMES TI
VII. FIRMES AVOCATS
VIII. FOURNISSEURS
IX. COMPÉTITEURS
X. CLIENTS
XI. PARTENAIRES D'AFFAIRES
XII. ASSOCIATIONS
XIII. RÉSEAUX
1. ASSOCIATIONS PROFESSIONNELLES
2. CONTACTS PERSONNELS
3. COMITÉS INTERENTREPRISES
4. PARTENARIATS PUBLIC-PRIVÉS

c. NATURE DES RELATIONS
I. CONFLIT/CONFRONTATION
II. COLLABORATION/COOPÉRATION
III. ÉCHANGE
IV. NÉGOCIATION
V. COMPROMIS/ACCOMODEMENT
VI. COMMUNICATION
VII. CONVAINCRE/INFLUENCER

3. PROFIL DU GESTIONNAIRE
a. RÔLE ET RESPONSABILITÉS
I. PARTICIPATIF/ACTIF
II. PASSIF/EXÉCUTANT
III. RECOMMANDATIONS
IV. IDENTIFICATION DES ACTIFS INFORMATIONNELS
V. CRÉATION DE SOLUTIONS ADAPTÉES
VI. GESTION DU CYBER-RISQUE
VII. GESTION DES IDENTITÉS/ACCÈS

VIII. ÉLABORATION DE PROCÉDURES/POLITIQUES
IX. GESTION DE PERSONNEL
X. SENSIBILISATION
XI. NÉGOCIATION
XII. GESTION DE CRISE
XIII. ENQUÊTE
XIV. COLLABORATION INTERDÉPARTEMENTALE

b. CHEMINEMENT DE CARRIÈRE
I. EXPÉRIENCE POLICIÈRE/MILITAIRE
II. EXPÉRIENCE MIXTE PUBLIQUE ET PRIVÉE
III. EXPÉRIENCE DIVERSES ORGANISATIONS
IV. ENSEIGNEMENT
V. NIVEAU D'ÉTUDES (COLLÉGIAL, UNIVERSITAIRE)
VI. AYANT EU UN MENTOR

c. PERSONNALITÉ
I. CONNAISSANCE
II. COMPÉTENCES TECHNIQUES
III. INTUITION
IV. VUE D'ENSEMBLE/RECUL
V. RESPECT
VI. CRÉDIBILITÉ/AUTORITÉ NON FORMELLE
VII. LEADERSHIP
VIII. SCOLARITÉ
IX. CAPITAL SOCIAL
X. MATURITÉ
XI. CONVAINCRE SANS CONFRONTATION
XII. HABILITÉS COMMUNICATIONNELLES

d. OUTILS/MESURES ADOPTÉS PAR LE GESTIONNAIRE DE LA SÉCURITÉ
I. CODE D'ÉTHIQUE
II. POLITIQUE DE CONFIDENTIALITÉ
III. GESTION DES ACCÈS/IDENTITÉS
IV. CLASSIFICATION DES ACTIFS INFORMATIONNELS
V. COMPARTIMENTATION DE L'INFORMATION
VI. FORMATION/SENSIBILISATION
VII. VÉRIFICATION PRÉ-EMPLOI
VIII. CHIFFREMENT DES DONNÉES
IX. ACTIVITÉS DE SURVEILLANCE/CONTRÔLES PÉRIODIQUES
X. ANALYSE QUANTITATIVE/MATRICE DE RISQUES

4. SOURCES D'INFORMATIONS
I. RÉSEAUX PROFESSIONNELS
II. RÉSEAUX PERSONNELS
III. COLLOQUES/CONFÉRENCES
IV. PÉRIODIQUES SCIENTIFIQUES, RECHERCHES, ÉTUDES
V. REVUES ET MAGAZINES SPÉCIALISÉS

VI. SITES HACKERS
VII. SITES FOURNISSEURS
VIII. STATISTIQUES DE L'ENTREPRISE
IX. VIGIE TECHNOLOGIQUE
X. PERSONNEL DE L'ENTREPRISE (EMPLOYÉS, CADRES, DIRECTION)
XI. AUDITS
XII. WEB
XIII. MÉDIAS