Engagement et pratiques des organisations en matière de gouvernance de la sécurité de l'information

Nathalie DAGORN & Nicolas POUSSING***

* ICN Business School Nancy-Metz, Laboratoire CEREFIGE
** CEPS/INSTEAD Esch-sur-Alzette (Luxembourg), Laboratoire CREM Rennes

RÉSUMÉ

Cet article aborde le thème de la gouvernance de la sécurité de l'information. Pour pallier les faiblesses relevées dans la littérature, il explore (i) le processus d'engagement des organisations dans la gouvernance de la sécurité de l'information et (ii) les pratiques des organisations engagées dans la démarche. L'analyse statistique et économétrique de données issues d'une enquête conduite auprès de cent vingt grandes entreprises luxembourgeoises suggère que la connaissance d'organisations engagées dans la gouvernance de la sécurité de l'information ou promouvant cette approche, la performance espérée et l'effort déployé sont des déterminants de l'engagement des organisations dans la démarche. Ces résultats peuvent être rapprochés du modèle unifié d'adoption des technologies (UTAUT) formulé par Venkatesh et al. (2003). Les données des organisations permettent aussi d'établir un état des pratiques actuelles en matière de gouvernance de la sécurité de l'information. L'originalité majeure de cette recherche réside dans le taux de participation très important (85,71%) des organisations à l'enquête menée, conférant aux résultats une forte validité, qui plus est, dans un domaine extrêmement sensible et confidentiel. Sur le plan théorique, la recherche améliore la connaissance du domaine sur les deux questions abordées. En pratique, elle fournit aux managers un retour sur les pratiques actuelles des organisations en matière de gouvernance de la sécurité de l'information et propose quelques recommandations. Ces contributions peuvent également avoir une incidence sur les politiques publiques et organismes promouvant la gouvernance de la sécurité de l'information.

Mots-clés : Engagement, Gouvernance, Pratiques, Sécurité de l'information, UTAUT.

ABSTRACT

This article looks at the issue of information security governance. To respond to the shortcomings identified in the literature, it explores (i) the process of organizations' engagement in the governance of information security, and (ii) the practices of the organizations involved. The statistical and econometric analysis of data from a survey conducted with one hundred and twenty large companies in Luxembourg suggests that the knowledge of organizations involved in the governance of information security or promoting this approach, the expected performance, and the effort undertaken, are potential determinants of the organizations' engagement in the process. These results may be analyzed under the unified theory of acceptance and use of technology (UTAUT) developed by Venkatesh et al. (2003). The data from organizations also helps to draw a picture of current practices in the matter of information security governance. The major originality of the research lies in the very high participation rate (85.71%) by organizations in the study, which gives the results a strong validity in what is, moreover, an extremely sensitive and confidential field. At the theoretical level, the research improves knowledge of the two issues explored. In practice, it provides managers with feedback on current practices implemented by the organizations in the field of information security governance and draws some recommendations. These contributions may also have an impact on public policies and on institutions promoting information security governance.

Keywords: Engagement, Governance, Practices, Information security, UTAUT.

INTRODUCTION

La gouvernance de la sécurité de l'information est une approche stratégique de la sécurité visant à la protection des actifs informationnels[1] de l'organisation, dans une acceptation allant bien au-delà de la « simple » garantie opérationnelle que les informations de l'organisation sont adéquatement protégées : elle implique une vision holistique du management de la sécurité de l'information, comprenant des enjeux, des décisions, une stratégie globale et à long terme qui ne font pas partie des missions du technicien. Ce postulat pour une gouvernance de la sécurité de l'information peut s'expliquer par les différentes initiatives de conformité (*compliance*) suscitées par les lois de sécurité financière récemment mises en place. En effet, les scandales financiers d'Enron, Worldcom et Parmalat il y a maintenant huit ans, ont propulsé la gouvernance institutionnelle et le contrôle interne parmi les priorités des organisations et des investisseurs. Les lois et réglementations en découlant (Sarbanes-Oxley aux Etats-Unis, Bâle II touchant les pays de l'OCDE, et la loi de sécurité financière en France) ont rapidement été appliquées dans la plupart des secteurs d'activité. Selon Moulton et Coles (2003) ainsi que Teufel (2003), celles-ci ont un impact significatif sur les technologies de l'information (TI) déployées dans les organisations, et en particulier sur le management de la sécurité puisqu'elles requièrent la mise en place dans les organisations de diverses mesures stratégiques de sécurité allant, pour les sociétés anonymes, de la présentation d'un rapport annuel sur les procédures de contrôle interne liées à la sécurité de l'information, à l'instauration, pour les professionnels du secteur financier, d'une véritable politique de gestion des risques génériques et fonctionnels. Cette posture impose une gestion des risques et une prise en compte des questions de sécurité de l'information au plus haut niveau de l'organisation. Dans ce contexte, la gouvernance de la sécurité de l'information prend tout son sens puisqu'elle « *consiste à mettre en place une structure permettant de prendre les bonnes décisions en matière de sécurité, au bon moment et au bon niveau hiérarchique* » (Fernandez-Toro, 2009, p. 91). Elle permet aux organisations d'inclure les questions de sécurité dans leur stratégie de gouvernance institutionnelle. Mais l'intérêt d'une gouvernance de la sécurité de l'information s'explique également par la prise de conscience grandissante des dirigeants, de l'impact profond que peuvent avoir les questions de sécurité sur le bon fonctionnement et la performance du système d'information (SI) de l'organisation.

Pour répondre à ces préoccupations, de nombreux référentiels de pratiques (CMMi, Cobit, Coso, Gtag, Itil, RiskIT) et normes internationales (suite ISO 27000, norme ISO 15408) incluent désormais des paragraphes sur la gouvernance de la sécurité. Les premiers

[1] Sapir (2005, p. 159) définit un actif informationnel comme « *une information considérée comme simultanément pertinente et utilisable pour une décision donnée* ».

rapports ou articles de revues académiques évoquant clairement la gouvernance de la sécurité de l'information datent du début des années 2000. Les contributions en sciences de gestion comprennent surtout des articles concernant l'organisation de la gouvernance de la sécurité (rôle du management, valeur stratégique). Cependant, à notre connaissance, la problématique de l'engagement des organisations dans cette démarche de gouvernance de la sécurité de l'information n'a pas encore été étudiée. De même, les pratiques actuelles de gouvernance de la sécurité de l'information ne sont que peu explicitées et mériteraient d'être actualisées. Notre recherche tente de répondre à ces interrogations.

L'article est structuré comme suit. La section 2 présente les travaux antérieurs ayant trait à la gouvernance de la sécurité de l'information dans la littérature académique (2.1) et clarifie les motivations de notre recherche (2.2). La section 3 décrit l'enquête conduite auprès de cent vingt grandes entreprises luxembourgeoises (3.1), restitue une image fidèle de leurs pratiques en matière de gouvernance de la sécurité de l'information *via* une analyse statistique (3.2) et suggère, *via* une analyse économétrique, trois déterminants du processus d'engagement des organisations dans la gouvernance de la sécurité de l'information (3.3). La section 4 analyse et discute les résultats de cette recherche (4.1) ; elle examine ses contributions théoriques, méthodologiques et pratiques (4.2), ses limites et dégage des pistes de recherches futures (4.3). Au vu de ces éléments, la section 5 énonce nos conclusions.

1. CADRE CONCEPTUEL

Cette section présente les travaux antérieurs sur le thème du management stratégique (ou gouvernance) de la sécurité dans la littérature académique et clarifie les motivations de notre recherche.

1.1. La gouvernance de la sécurité de l'information dans la littérature

En sciences de gestion, les responsabilités et rôles du management, et en particulier de la direction générale, sont mis en avant par plusieurs auteurs. Ainsi, Straub et Welke (1998) postulent que le risque de sécurité concernant le SI peut être réduit lorsque les managers sont conscients de l'étendue des contrôles existants et mettent en œuvre les contrôles les plus efficaces en fonction des risques identifiés. Williams (2001), alors président de l'ISACA et co-fondateur de l'IT Governance Institute, rappelle que les directeurs des organisations ont la responsabilité de protéger la valeur actionnariale, et que cette responsabilité s'applique aux actifs informationnels valorisés. Rockart et Crescenzi (1984), Davenport (2002) et Reix (2004) insistent sur la nécessité de considérer la sécurité de l'information comme un problème de managers et non de techniciens ; Markus (1983), de même que Knapp *et al.* (2006, 2009), confirment que la sécurité doit être prise en compte au niveau de la direction générale de l'organisation. Williams (2007) précise les rôles de la direction et du conseil d'administration en matière de sécurité de l'information.

Plusieurs auteurs ont étudié la valeur ajoutée, l'avantage stratégique et/ou concurrentiel procurés par la mise en place d'une gouvernance de la sécurité de l'information. En ce sens, Williams (2001) postule que les actifs informationnels sont essentiels à la survie de l'organisation et susceptibles de générer un avantage concurrentiel. Schou et Schoemaker (2006) constatent que, pour procurer un avantage plus important à l'organisation, la gouvernance de la sécurité de l'information peut éventuellement être coordonnée avec des démarches stratégiques d'intelligence économique, de responsabilité sociétale ou de communication. Shi-Ming *et al.* (2006) s'appuient sur un tableau de bord équilibré pour mettre en place dans les organisations des indicateurs de performance pour le management de la sécurité de l'information, et renforcer le lien entre ces indicateurs et la stratégie institutionnelle. Kraemer *et al.* (2009) montrent que les facteurs humains et organisationnels jouent un rôle significatif dans le développement des vulnérabilités liées au SI et suggèrent une approche multiniveau pour améliorer la performance de la sécurité du SI. Johnston et Hale (2009) examinent les aspects stratégiques de la sécurité de l'information et essaient d'évaluer la valeur ajoutée apportée à l'organisation par la démarche de gouvernance de la sécurité ; les auteurs proposent un plan de sécurité de l'information fondé sur une enquête menée auprès de professionnels de la sécurité, ainsi que des programmes pour sa mise en œuvre. Pour Krjukovs et Strauss (2009), la valeur ajoutée et la performance sont deux éléments cruciaux de la gouvernance de la sécurité de l'information.

Enfin, parmi les autres contributions, Dhillon *et al.* (2007) présentent les résultats d'une étude empirique permettant de mieux comprendre les dimensions de la gouvernance de la sécurité des SI. Dans son ouvrage sur la gouvernance de la sécurité de l'information, Brotby (2009) consacre plusieurs chapitres aux rôles et responsabilités des managers, aux mesures stratégiques et avantages de la démarche, au développement et à la mise en œuvre d'une stratégie de gouvernance de la sécurité de l'information et de gestion des incidents. Klai (2010) discute la nécessité de définir un niveau de gouvernance dans l'organisation et clarifie le lien existant entre ce niveau et les programmes de sécurité.

1.2. Motivations de notre recherche

Notre revue de littérature suggère que la sécurité de l'information est passée progressivement d'une dimension opérationnelle à une dimension stratégique. Les contributions antérieures ont proposé divers modèles pour la gouvernance de la sécurité de l'information, discuté le rôle du management et la valeur ajoutée de cette démarche. Mais il apparaît que la question de l'engagement des organisations dans le processus de gouvernance de la sécurité de l'information n'a pas encore été étudiée.

Par ailleurs, au sein de la communauté académique, des difficultés sont régulièrement rapportées par les

chercheurs en sécurité, tant pour l'élaboration de théories (par exemple, par Dhillon & Backhouse, 2001; Dlamini *et al*., 2009) qu'en matière de recherches empiriques (les faibles taux de participation aux études en témoignent) ; hormis quelques études de cas, les enquêtes recensant les pratiques détaillées d'un échantillon significatif d'organisations en matière de gouvernance de la sécurité de l'information sont rares. Il nous semble qu'un état des pratiques courantes des organisations, établi à partir de nouvelles données, actualiserait les connaissances dans ce champ de recherche.

Nous nous proposons donc de répondre ici à deux questions :

- quels sont les facteurs déterminant l'engagement des organisations dans la gouvernance de la sécurité de l'information ?
- quelles pratiques de gouvernance de la sécurité de l'information sont mises en œuvre par les organisations engagées dans la démarche ?

2. ÉTUDE EMPIRIQUE

Afin de répondre aux questions de recherche posées, nous exploitons (analyse statistique et économétrique) des données collectées dans le cadre d'une enquête menée auprès de grandes entreprises implantées au Luxembourg. Les paragraphes suivants présentent la méthodologie de recherche mise en œuvre et les résultats obtenus.

2.1. Données et méthodologie

2.1.1. La collecte des données

Nos données ont été collectées auprès de grandes entreprises luxembourgeoises. Ce choix trouve plusieurs justifications. La gouvernance a été mise en œuvre d'abord par les grandes entreprises (Pougnet-Rozan, 2005 ; IT Governance Institute, 2006). Dans le même ordre d'idée, Waddock et Graves (1997) démontrent que les organisations disposant de ressources financières importantes peuvent davantage investir dans des activités stratégiques, or les ressources financières et les compétences se trouvent généralement dans les maisons-mères ou structures les plus importantes (Archibugi & Michie, 1994). Elles sont ensuite diffusées aux filiales du groupe (Bartlett & Ghoshal, 1991). Cohen (2006) précise que les organisations doivent prendre en compte la dimension de la sécurité dans leur stratégie lorsqu'elles évoluent dans un environnement compétitif, ce qui est souvent le cas des grandes entreprises. Par ailleurs, les PME font état, depuis toujours, d'un manque global de sensibilisation à la sécurité (Mitchell *et al.,* 1999) et sont confrontées à des problèmes plus importants que ceux rencontrés par les grandes entreprises en matière de sécurité : difficultés de recrutement de personnes qualifiées (Monnoyer, 2003) et d'appréciation réaliste des risques encourus (Boulet, 2007 ; Goodhue & Straub, 1991). Les dirigeants des PME se préoccupent peu des questions de sécurité (Barlette, 2009, 2011; Carpentier, 2009 ; Gupta & Hammond, 2005) et la grande

majorité des PME n'a aucune obligation légale en matière de sécurité à ce jour (Barlette, 2011). La sécurisation des PME accuse donc toujours un retard sur les grandes entreprises (Clusif, 2010). Enfin, nous avons interrogé des organisations implantées au Luxembourg car des travaux récents mettent en avant la disposition favorable des grandes entreprises envers les TI et la sécurité au Grand-duché, particulièrement dans le secteur financier (Martin & Poussing, 2007, 2008a, 2008b).

Pour sélectionner les organisations cibles, nous nous sommes référés au répertoire des entreprises édité par l'Institut national de la statistique et des études économiques du Luxembourg (STATEC[2]). Cette liste renseigne le nom et/ou la dénomination des organisations implantées au Luxembourg, leur secteur d'activité et leur taille (en nombre de salariés). Nous avons ainsi identifié cent quarante organisations de deux cent cinquante salariés et plus. Par des recherches sur Internet et des contacts téléphoniques, nous avons rassemblé leurs coordonnées complètes ainsi que celles de leur responsable de la sécurité. Ces organisations appartiennent à la quasi-totalité des secteurs d'activité : la construction, le transport, les télécommunications et l'informatique[3], l'industrie, le commerce, les services et la finance. Cette décomposition sectorielle est conforme à la nomenclature européenne des activités économiques (NACE rev. 1) habituellement utilisée dans la cadre des enquêtes communautaires.

Le questionnaire véhiculé a été réalisé en plusieurs étapes. Une première version a été élaborée afin de prendre en considération nos hypothèses théoriques. Cette première version a été testée auprès de deux responsables de la sécurité. Ce prétest a permis de reformuler certaines questions afin d'améliorer la compréhension du questionnaire et par là-même d'améliorer la qualité des réponses données (élimination de la non-réponse partielle). Au final, le questionnaire comprend trente questions réparties en six thèmes : la connaissance de la gouvernance de la sécurité de l'information, ses enjeux stratégiques, ses conditions de mise en œuvre, son niveau de maturité, son mode d'organisation et les caractéristiques économiques des organisations répondantes. Le questionnaire a été rédigé dans les trois langues les plus pratiquées au sein des organisations implantées au Luxembourg, à savoir le français, l'anglais et l'allemand (les questionnaires sont disponibles sur demande).

La collecte des données a été réalisée durant le dernier trimestre 2010. Elle s'est déroulée en deux temps. D'abord, le questionnaire a été envoyé par courrier, messagerie électronique ou remis en mains propres aux responsables de la sécurité des organisations cibles dans la langue de leur choix afin d'être complété par leurs

[2] http://www.statistiques.public.lu/fr/acteurs/statec/index.html.

[3] Les organisations du secteur informatique sont éliminées des échantillons lorsqu'elles sont susceptibles de biaiser les résultats concernant des comportements ou des connaissances « techniques » ; nous ne les avons pas soustraites de notre échantillon car, justement, il ne s'agit pas de tester ici des hypothèses techniques mais managériales.

soins. Puis il nous a été restitué par les organisations à l'occasion d'un rendez-vous qui a permis de vérifier que le répondant avait bien répondu à toutes les questions et, dans la négative, de lui donner les explications permettant de compléter ses réponses. Nous avons ainsi obtenu cent vingt réponses exploitables, soit un taux de réponse de 85,71%. Vingt organisations n'ont pas donné suite à notre demande, principalement pour des raisons de confidentialité des informations de sécurité[4].

2.1.2. Les caractéristiques de la population étudiée

Notre population est composée de 31% d'organisations appartenant au secteur des services, 22% au secteur financier, 19% à l'industrie. La construction, les transports et le commerce représentent respectivement 12%, 7% et 7% des organisations de notre population. La proportion d'organisations appartenant au secteur des télécommunications est de 2% (Annexe A). 72% des organisations appartiennent à un groupe (29% sont des maisons-mères et 43% des filiales). La plupart des organisations (67%) évolue sur le marché extranational (européen pour 16% et international pour 51%). La moitié des organisations de la population (49%) a vu son chiffre d'affaires augmenter durant les trois dernières années ; pour 42% d'entre elles, il est resté stable ou a diminué. Les répondants à l'enquête assurent des fonctions de responsable SI/TI (DSI), *risk manager*, directeur général, responsable qualité/conformité, RSSI ou *security officer*. L'âge des répondants varie entre 22 et 62 ans (avec une moyenne de 42 ans). Le niveau d'études des répondants varie du Bac au Bac+8 ; 37% ont un niveau d'études supérieur ou égal à Bac+5.

2.1.3. Le modèle mis en œuvre

Dans un premier temps, des statistiques descriptives permettent de présenter les pratiques détaillées des organisations interrogées.

Dans un deuxième temps, afin de mettre au jour les déterminants du processus d'engagement des organisations dans une démarche de gouvernance de la sécurité de l'information, nous avons choisi de mettre en œuvre une analyse multivariée. Ce choix trouve sa motivation dans le fait que nous serons ainsi en mesure d'isoler l'influence de la variation d'une caractéristique, à l'exclusion de tout autre facteur (analyse toutes choses égales par ailleurs) sur la probabilité de s'engager dans une démarche de gouvernance de la sécurité de l'information ou non.

Devant modéliser le fait de s'engager ou de ne pas s'engager dans une démarche de gouvernance de la sécurité de l'information, nous constatons l'absence de continuité dans les modalités prises par la variable expliquée. S'engager ou ne pas s'engager dans une telle démarche est une variable binaire qui prend la valeur 1 pour une réponse positive et la valeur 0 pour une ré-

[4] Problème de confidentialité (65%), organisation peu informatisée ou externalisation (20%), contact non intéressé (15%).

ponse négative. Cette caractéristique de la variable expliquée impose l'utilisation de méthodes spécifiques, en l'occurrence de modèles dichotomiques simples Logit et Probit.

Au sein de notre population de cent vingt organisations i (i étant compris entre 1 et 120), on observe pour chaque organisation la survenance d'un événement y_i où :

y_i = 1 si l'organisation i s'engage dans une démarche de gouvernance de la sécurité de l'information,

y_i = 0 si l'organisation i ne s'engage pas dans une telle démarche.

Les modèles dichotomiques admettent pour variable expliquée que la probabilité d'apparition de cet événement est conditionnelle aux variables exogènes. Le modèle prend la forme suivante :

$$p_i = \text{Prob}\,(y_i = 1 \mid x_i) = F\,(x_i\beta)$$

où la fonction F (.) désigne une fonction de répartition, x_i désigne les variables explicatives et β le vecteur des paramètres à estimer.

Si y_i^* est une variable latente (inobservable) qui est fonction des variables explicatives (x_i), du vecteur des paramètres à estimer (noté β) et du terme d'erreur (noté ε_i), la règle de décision probabiliste s'écrit alors :

$$\text{Prob}\,(y_i=1) = \text{Prob}\,(y_i^* > 0) = 1\text{-}F\,(-\beta x_i) = F\,(\beta x_i)$$

$$\text{Prob}\,(y_i=0) = \text{Prob}\,(y_i^* \leq 0) = F\,(-\beta x_i) = 1 - F\,(\beta x_i)$$

où β est le vecteur des coefficients estimés et F (.) est la fonction de répartition.

La fonction de répartition F (.) peut être de deux types : soit une loi logistique (modèle Logit), soit une loi normale centrée réduite (modèle Probit). Les résultats obtenus à partir des modèles Probit et Logit sont relativement similaires (Morimune, 1979 ; Davidson & MacKinnon, 1984). Pour nos estimations, nous retiendrons un modèle Logit où l'estimation des paramètres du modèle est réalisée par la méthode du maximum de vraisemblance.

La population d'analyse étant de taille modeste (cent vingt organisations), le nombre de variables explicatives introduites dans nos modèles devra être limité. Afin de lever cette contrainte, nous avons agrégé les modalités de certaines variables. Pour tirer profit de la richesse du questionnaire, nous avons créé des variables qui synthétisent les informations disponibles et réalisé plusieurs estimations où toutes les informations disponibles sont introduites alternativement. Plus précisément, les secteurs d'activité ont été regroupés en deux secteurs : industrie *versus* service (variables INDUS et SERV)[5]. Pour prendre en compte la variation du chiffre d'affaires durant les trois der-

[5] Compte tenu de l'importance du secteur de la finance au Luxembourg, l'appartenance à tel ou tel secteur d'activité a aussi été prise en compte à l'aide de trois modalités : appartenir à l'industrie, appartenir au secteur de la finance, appartenir à un autre secteur. Les résultats obtenus avec cette spécification montrent que l'appartenance au secteur de la finance est sans effet sur la probabilité de s'engager dans une gouvernance de la sécurité de l'information. Réduire l'appartenance sectorielle à deux secteurs (industrie *versus* service) est donc sans impact sur nos résultats.

nières années, nous nous focalisons sur l'impact d'un chiffre d'affaires en croissance (variable CHIDA).

Afin que la façon dont sont construites les variables n'affecte pas nos estimations, certaines caractéristiques sont prises en compte à l'aide de différentes variables. Ainsi, la connaissance de structures engagées dans une démarche de gouvernance de la sécurité est prise en compte alternativement de quatre façons :

- à l'aide du nombre de structures engagées dans une démarche de gouvernance de la sécurité que l'organisation connaît, compris entre 0 et 5 (variable NB_RESEAU) ;
- à l'aide de deux variables : connaître des clients ou des fournisseurs ou des concurrents engagés dans une démarche de gouvernance de la sécurité (variable RESEAU10) d'une part ; connaître d'autres organisations engagées dans une démarche de gouvernance de la sécurité, implantées au Luxembourg ou dans d'autres pays (variable RESEAU11) d'autre part ;
- à l'aide de trois variables : connaître des clients ou des fournisseurs engagés dans une démarche de gouvernance de la sécurité (variable RESEAU20) ; connaître des concurrents engagés dans une démarche de gouvernance de la sécurité (variable RESEAU21) ; connaître d'autres organisations, implantées au Luxembourg ou dans d'autres pays, engagées dans une démarche de gouvernance de la sécurité (variable RESEAU22) ;
- à l'aide d'une variable : connaître des organismes de promotion de la démarche de gouvernance de la sécurité (variable ORGANISME).

Pour prendre en compte les bénéfices, les obstacles et les domaines prioritaires d'une démarche de gouvernance de la sécurité de l'information, nous introduisons alternativement chaque bénéfice, obstacle et domaine prioritaire. Nous avons également construit trois variables qui prennent en compte le nombre de bénéfices retirés d'une démarche de gouvernance de la sécurité de l'information (NB_BENEF), le nombre d'obstacles rencontrés (NB_OBST) et le nombre de domaines prioritaires (NB_VAL).

L'ensemble des variables introduites dans notre modèle est présenté dans l'Annexe B[6].

2.2. Pratiques des organisations interrogées

Ce paragraphe présente les pratiques détaillées des organisations interrogées en matière de gouvernance de la sécurité de l'information à l'aide de statistiques descriptives, répondant ainsi à notre deuxième question de recherche.

2.2.1. Connaissance de la gouvernance de la sécurité de l'information

L'enquête révèle que 86% des organisations connaissent les pratiques de gouvernance des SI/TI et de la sécurité de l'information, essentiellement par

[6] L'existence de corrélation entre les variables a été testée. La matrice des corrélations n'a pas été introduite dans l'article pour ne pas alourdir la lecture. Elle peut être transmise sur demande.

le biais d'Internet, de formations professionnelles et de la veille technologique. 72% de ces organisations sont engagées à la fois dans une démarche de gouvernance des SI/TI et dans une démarche de gouvernance de la sécurité de l'information (Figure 1). 80% des organisations connaissent d'autres organisations engagées dans une démarche de gouvernance de la sécurité de l'information, dont 34% parmi leurs clients, 59% parmi leurs fournisseurs et 41% parmi leurs concurrents (Figure 2). Soixante-dix-sept de ces organisations (80%) sont engagées dans la démarche de gouvernance de la sécurité de l'information. Une large proportion d'organisations connaît également d'autres organisations luxembourgeoises (62%) et étrangères (57%) engagées dans une démarche de gouvernance de la sécurité de l'information. 42% des organisations connaissent des organismes luxembourgeois ou étrangers cherchant à promouvoir la gouvernance de la sécurité de l'information (par exemple, le Clusil, le centre de recherche public Henri Tudor, la

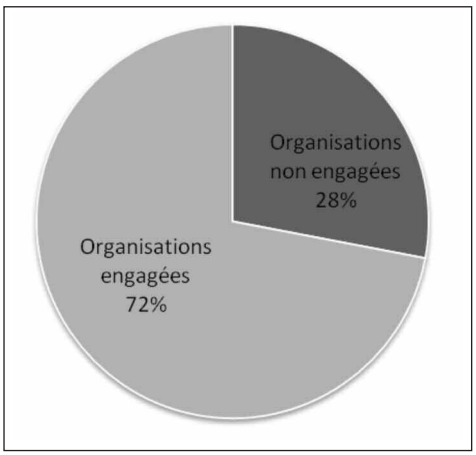


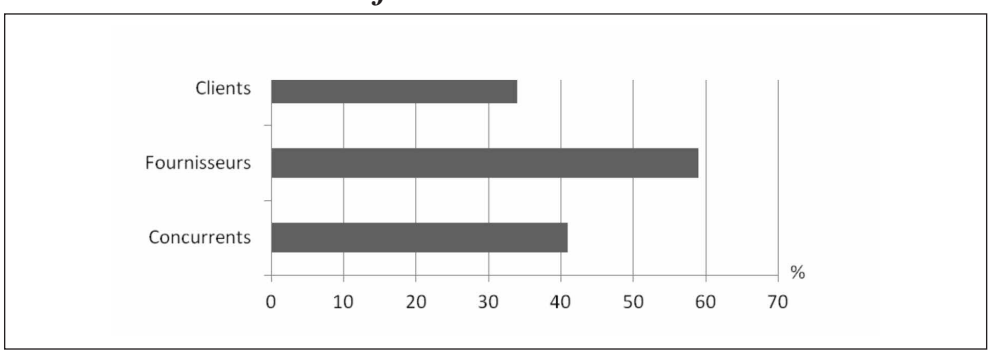
Figure 1. Engagement des organisations dans une démarche de gouvernance de la sécurité de l'information

CSSF[7] au Luxembourg, l'ISACA en France ou le BSI[8] en Allemagne).

2.2.2. Enjeux stratégiques de la gouvernance de la sécurité de l'information

Au sein des organisations pratiquant la gouvernance de la sécurité de l'in-

Figure 2. Connaissance d'organisations pratiquant la gouvernance de la sécurité de l'information dans l'environnement



[7] CLUb de la Sécurité de l'Information Luxembourg, http://www.clusil.lu/; http://www.tudor.lu/; Commission de Surveillance du Secteur Financier, http://www.cssf.lu/.

[8] *Bundesamt für Sicherheit in der Informationstechnik*, https://www.bsi.bund.de/.

formation, sa mise en œuvre résulte avant tout de la nécessité de satisfaire les clients (72%). Elle vise ensuite à contenter les actionnaires et la direction (48%), les salariés (40%), la législation en vigueur (36%), les fournisseurs (17%), les collectivités locales ou organisations non gouvernementales (12%). Les principaux bénéfices et obstacles rencontrés ou perçus de la gouvernance de la sécurité de l'information sont synthétisés dans une matrice SWOT (Annexe C), qui fournit une analyse stratégique des forces (*strengths*), faiblesses (*weaknesses*), opportunités (*opportunities*) et menaces (*threats*) liées à la démarche. 95% des organisations pensent pouvoir retirer un avantage concurrentiel (bénéfices très importants ou importants) de la gouvernance de la sécurité de l'information et 75% d'entre elles sont engagées dans la démarche. Parmi treize bénéfices jugés très importants retirés de la gouvernance de la sécurité de l'information, les organisations mettent principalement en avant l'amélioration des procédures en matière de sécurité (52%), la conformité avec la législation (32%) et le gage de confiance pour les partenaires (31%) ; ces résultats sont illustrés par la Figure 3. *A contrario*, 94% des organisations interrogées perçoivent des difficultés (obstacles très importants ou importants) dans la mise en œuvre de la gouvernance de la sécurité de l'information, pourtant 74% d'entre elles sont engagées dans la démarche. L'examen des obstacles jugés très importants par les organisations fait apparaître, par ordre de citation décroissant, le manque de temps (21%), le manque de ressources en interne (20%), le coût de la mise en œuvre (17%) et le manque d'intérêt de la Direction (17%) ; ces résultats sont illustrés par la Figure 4. Dans les organisations pratiquant la gouvernance de la sécurité de l'information, les bénéfices de cette démarche sont jugés très supérieurs aux coûts pour 15% d'entre elles, légèrement supérieurs aux coûts pour 14%, globalement équivalents aux coûts pour 17%, légèrement inférieurs aux coûts pour 13% et très inférieurs aux coûts pour 8%. 33% des répondants ne savent pas estimer précisément les bénéfices retirés de la démarche. Au sein des organisations pratiquant la gouvernance de la sécurité de l'information, la responsabilité de cette démarche est confiée à un responsable SI/TI (DSI) pour 53% d'entre elles, à un *risk manager* pour 14%, au directeur de l'organisation pour 13%, à un responsable qualité/conformité

Figure 3. Principaux bénéfices retirés de la gouvernance de la sécurité de l'information

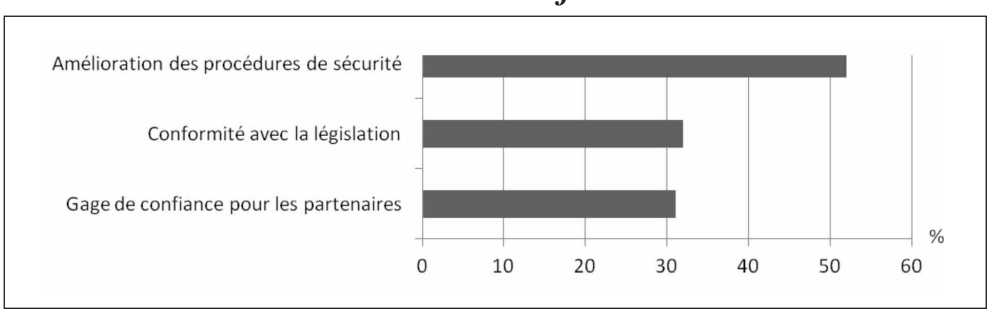
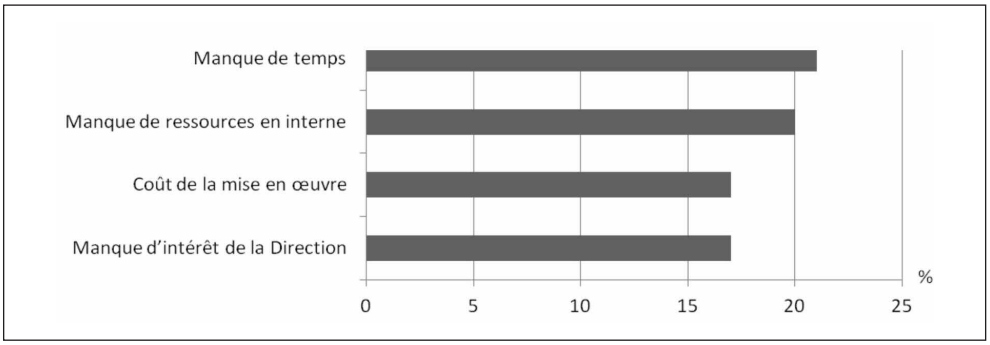


Figure 4. Principaux obstacles à la mise en œuvre de la gouvernance de la sécurité de l'information



pour 12% et à un RSSI (ou *security officer*) dans seulement 8% des cas.

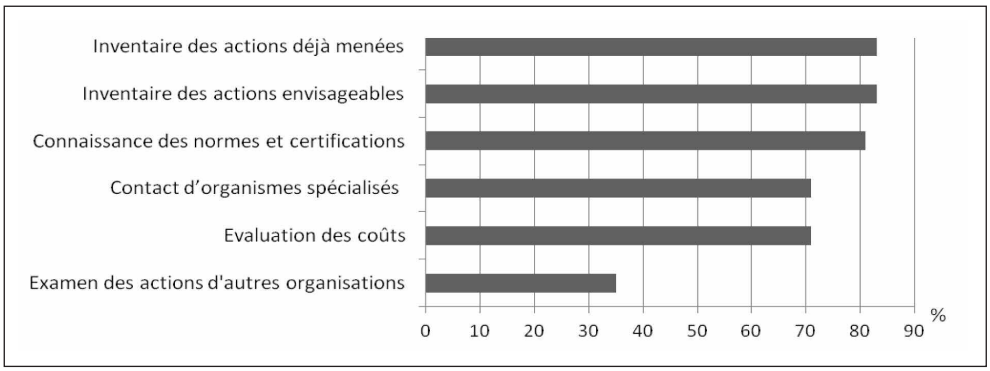
2.2.3. Conditions de mise en œuvre de la gouvernance de la sécurité de l'information

Avant d'engager une démarche de gouvernance de la sécurité de l'information, les organisations pratiquantes ont fait l'inventaire des actions déjà menées en interne (83%) ainsi que des actions envisageables (83%), pris connaissance des normes et certifications existantes (81%), collecté des informations auprès d'organismes spécialisés (71%), évalué les coûts de mise en œuvre de la démarche (71%) et examiné les actions menées par d'autres organisations (35%) ; ces résultats sont illustrés par la Figure 5. En moyenne 6 personnes par organisation sont affectées à la démarche de gouvernance de la sécurité de l'information dont 2 responsables, 3 membres de l'équipe SI/TI, 1 consultant externe ou autre (par exemple, un salarié de la maison-mère ou un correspondant métiers). Presque une organisation sur deux (45%) dispose d'un budget dédié à la sécurité de l'information. La mise en œuvre de la gouvernance de la sécurité de l'information est décrite et valorisée par 27% des organisations dans leur rapport d'activités, par 16% sur leur site Web, par 45% dans leurs documents internes (intranet, charte informatique), nulle part pour 29% d'entre elles. De même 63% des organisations ont établi des plans de communication de leurs engagements en interne, 17% vers l'extérieur et 34% n'ont pas du tout communiqué sur ces engagements.

2.2.4. Organisation de la gouvernance de la sécurité de l'information

Selon les organisations répondantes, les domaines prioritaires (ou valeurs) d'une démarche de gouvernance de la sécurité de l'information sont le management du risque et la réduction des impacts potentiels à un niveau acceptable (87%), l'alignement de la sécurité de l'information sur la stratégie institutionnelle (83%), les choix technologiques liés à la sécurité (78%), l'évaluation de la performance par le suivi d'indicateurs de sécurité (65%), le management des ressources information-

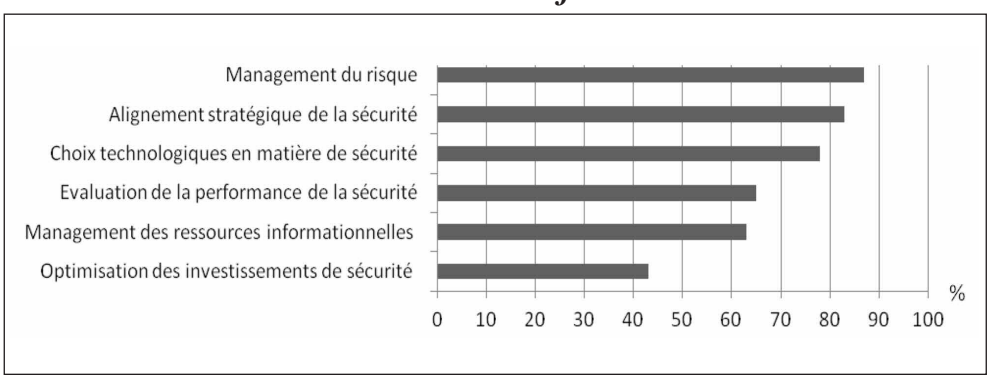
Figure 5. Démarches préalables à la mise en œuvre de la gouvernance de la sécurité de l'information



nelles (63%) et la création de valeur par l'optimisation des investissements de sécurité (43%) ; ces résultats sont illustrés par la Figure 6.

Parmi les organisations pratiquant la gouvernance de la sécurité de l'information, 41% se sont fixé des objectifs mesurables, par exemple la diminution des incidents de sécurité, la réduction du risque opérationnel, la mise en place d'un audit annuel, etc. 41% disposent d'outils permettant d'évaluer les effets de la démarche de gouvernance appliquée, tels que l'analyse des causes premières, le scanner de vulnérabilités, divers outils de surveillance informatique, etc. 33% ont mis en place un tableau de bord pour suivre leur plan de gouvernance de la sécurité de l'information par des indicateurs-clés de performance (KPI pour *Key Performance Indicators*). 62% ont élaboré des plans d'actions, en cours ou futurs, dans le cadre de la gouvernance de la sécurité de l'information, comprenant par exemple la mise en place d'un plan de continuité des activités, la formation du personnel, la redondance du réseau informatique, la centralisation des données, la virtualisation des serveurs, l'amélioration de la traçabilité, etc.

Figure 6. Domaines prioritaires d'une démarche de gouvernance de la sécurité de l'information



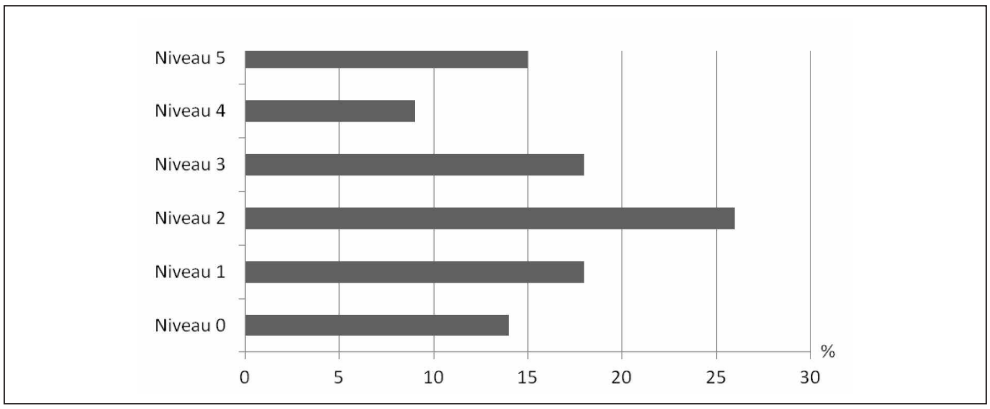
2.2.5. Maturité des organisations en matière de gouvernance de la sécurité de l'information

Au total 48% des organisations interrogées jugent la gouvernance de la sécurité de l'information indispensable ; 38% la considèrent nécessaire, 9% peu utile et 4% inutile. 87% des responsables interrogés perçoivent donc la gouvernance de la sécurité de l'information comme une valeur importante pour l'organisation ; 79% de ces organisations sont engagées dans une démarche de gouvernance de la sécurité de l'information. En analysant la maturité des organisations en matière de gouvernance de la sécurité de l'information selon une typologie proposée par l'IT Governance Institute (2006), il apparaît que :

- pour 14% aucune procédure n'est appliquée. L'organisation ne reconnaît aucun besoin en matière de sécurité de l'information. Aucune obligation ni responsabilité n'est établie. Ceci correspond au niveau de base (niveau 0) ;
- pour 18% des procédures existent mais restent désorganisées. Les risques TI sont appréciés *ad hoc* par projet. L'organisation reconnaît le besoin de sécuriser ses ressources informationnelles, mais de manière réactive. Les responsabilités sont informelles. Ceci correspond au niveau 1 ;
- pour 26% les procédures suivent un modèle défini. Les risques TI sont jugés importants. Des politiques de sécurité sont en cours de développement. Le rapport *(reporting)* est incomplet ou inadéquat. Ceci correspond au niveau 2 ;
- pour 18% les procédures sont formalisées, documentées et communiquées par une politique organisationnelle. Le rapport reste axé sur les TI plutôt que sur l'organisation. Ceci correspond au niveau 3 ;
- pour 9% les procédures sont contrôlées et mesurées. La fonction sécurité est assurée par un manager senior. Les responsabilités sont appliquées. Le rapport est lié aux objectifs de l'organisation. Ceci correspond au niveau 4 ;
- pour 15% les procédures, technologies de sécurité et plans de secours sont intégrés dans l'activité de l'organisation, optimisés et automatisés. Le rapport permet d'anticiper les risques. Ceci correspond au niveau 5.

Ces résultats sont illustrés par la Figure 7. Le portefeuille de projets de gouvernance de la sécurité de l'information ne comprend aucun projet pour 28% des organisations interrogées ; des projets sont envisagés pour 33% d'entre elles (en moyenne 2 projets par organisation) ; des projets sont en cours pour 49% des organisations (en moyenne 3 projets par organisation) et des projets ont été clôturés durant les trois dernières années pour 35% d'entre elles (en moyenne 5 projets par organisation). 90% des organisations ayant engagé une démarche de gouvernance de la sécurité de l'information font état de mutations organisationnelles : recrutement de profils managériaux en externe (20%), évolution des métiers en interne pour 62%

Figure 7. Maturité des organisations sollicitées selon la typologie de l'IT Governance Institute (2006)



(par exemple, évolution des profils techniques vers des tâches managériales, spécialisation), mise en œuvre de formations spécifiques pour 66%, adaptation des départements pour 6% (par exemple, séparation TI/gestion des risques, mise en place ou révision de procédures de secours).

2.3. Les déterminants du processus d'engagement

Afin de répondre à notre première question de recherche, ce paragraphe présente les déterminants du processus d'engagement des organisations dans une démarche de gouvernance de la sécurité de l'information, mis au jour à l'aide de plusieurs spécifications de notre modèle économétrique (modèle Logit). Comme précisé plus avant, estimer plusieurs modèles permet d'introduire les potentiels déterminants de différentes façons afin de garantir la qualité des effets obtenus.

Le modèle 1 (cf. Annexe D) met en évidence l'impact positif du nombre de bénéfices attendus d'une démarche de gouvernance de la sécurité de l'information sur la probabilité d'adopter une telle démarche. On constate également que le nombre d'organisations que l'on sait avoir adopté une démarche de gouvernance de la sécurité de l'information a un effet positif sur la probabilité d'adopter ce type de gouvernance. En revanche, les caractéristiques économiques de l'organisation (son secteur d'activité, la croissance de son chiffre d'affaires, l'appartenance à un groupe) sont sans effet. Le nombre d'obstacles jugés importants est sans effet.

Pour affiner ce dernier résultat, nous avons introduit successivement et alternativement les différents obstacles rencontrés par les organisations[9]. Nous constatons alors que seuls deux obstacles ont un effet significatif : la difficulté à traduire les concepts en actions concrètes est un frein à l'adoption

[9] Lors de l'introduction dans nos modèles des variables prenant en compte les différents obstacles, bénéfices et valeurs, les tableaux de résultats ne mentionnent que les effets significatifs.

d'une gouvernance de la sécurité de l'information (modèle 2) ; le faible intérêt de la Direction pour les questions liées à la sécurité de l'information a également un impact négatif (modèle 3). La prise en compte simultanée de ces deux obstacles confirme uniquement l'effet négatif de la difficulté à traduire les concepts en actions concrètes (modèle 4).

L'ensemble des modèles (modèles 1 à 7) montre que le nombre de valeurs partagées par l'organisation relevant de la démarche de gouvernance de la sécurité de l'information n'affecte pas son adoption. Lorsque les valeurs jugées importantes par l'organisation sont prises en compte successivement, ce résultat persiste.

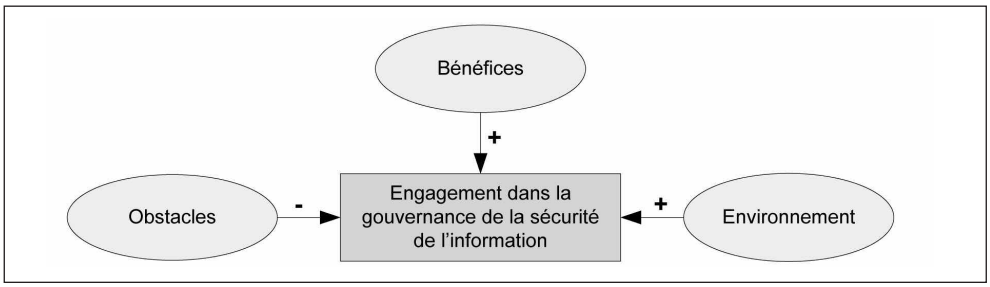
Une analyse détaillée de l'impact de l'environnement de l'organisation (connaître une organisation ayant une démarche de gouvernance de la sécurité de l'information ; connaître un organisme qui cherche à la promouvoir) montre que l'environnement de l'organisation a un effet positif sur la probabilité d'adopter une telle démarche, quelle que soit la manière de prendre compte cette dimension. D'une manière générale (modèles 5 à 7), on retrouve globalement les effets obtenus dans le modèle que l'on pourrait qualifier de base (modèle 1) : la croissance du chiffre d'affaires et le nombre de valeurs de l'organisation sont sans effet ; on peut également considérer que l'appartenance à un groupe est sans effet car seul le modèle 7 met en évidence un effet positif mais à un niveau très peu significatif (au seuil de 10%) ; le nombre de bénéfices a un effet incitatif sur l'adoption de la gouvernance de la sécurité de l'information et la difficulté à traduire les concepts en actions concrètes a un effet négatif. Connaître des clients ou des fournisseurs ou des concurrents, d'une part, et connaître d'autres organisations implantées au Luxembourg ou à l'étranger d'autre part, a un effet positif sur l'adoption d'une démarche de gouvernance de la sécurité de l'information (modèle 5). Lorsqu'on examine séparément les clients et les fournisseurs d'un côté et les concurrents de l'autre (modèle 6), on constate que connaître des clients ou des fournisseurs est sans effet ; connaître des concurrents et d'autres organisations engagés dans une démarche de gouvernance de la sécurité est faiblement significatif (au seuil de 10%). Connaître des organismes qui visent à promouvoir une telle démarche a un effet incitatif sur son adoption (modèle 7). Nous devons remarquer que cette spécification (modèle 7) met au jour un effet sectoriel : appartenir au secteur de l'industrie, relativement au secteur des services, affecte négativement la probabilité d'adopter une démarche de gouvernance de la sécurité de l'information. L'ensemble de ces résultats démontre l'effet incitatif de l'environnement de l'organisation sur son comportement.

Sachant que le nombre de bénéfices retirés d'une démarche de gouvernance de la sécurité a un effet positif sur la probabilité d'adoption de celle-ci (modèles 1 à 7), nous avons introduit successivement chaque bénéfice jugé important par l'organisation afin d'identifier le ou les bénéfices ayant un impact positif (cf. Annexe A). Force est de constater qu'aucun bénéfice n'a un effet significatif sur la probabilité d'adopter une démarche de gouver-

Tableau 1. Présentation synoptique des déterminants de l'engagement des organisations dans la gouvernance de la sécurité de l'information

Effet positif	Effet négatif
– Bénéfices : nombre de bénéfices retirés d'une gouvernance de la sécurité de l'information – Environnement : connaissance d'organisations engagées dans une gouvernance de la sécurité de l'information, connaissance d'organismes de promotion de la gouvernance de la sécurité de l'information	– Obstacles : difficulté à traduire les concepts en actions concrètes, appartenir au secteur de l'industrie comparativement au secteur des services

Figure 8. Déterminants proposés du processus d'engagement des organisations dans la gouvernance de la sécurité de l'information



nance de la sécurité de l'information[10]. Ce résultat montre que c'est l'accumulation de différents bénéfices jugés importants qui incite les organisations à s'inscrire dans une telle démarche et non l'impact d'un bénéfice en particulier.

En résumé, la probabilité d'adopter une démarche de gouvernance de la sécurité de l'information est affectée positivement par le nombre de bénéfices retirés d'une telle démarche, par la connaissance de structures engagées dans cette démarche (organisations ayant mis en œuvre cette démarche et organismes de promotion de celle-ci). Parmi une dizaine d'obstacles pouvant être rencontrés par les organisations, la difficulté de traduire les concepts en actions concrètes est la seule qui affecte négativement la probabilité d'adopter une démarche de gouvernance de la sécurité de l'information. Appartenir au secteur de l'industrie, comparativement au secteur des services, impacte négativement cette probabilité. Les autres caractéristiques des organisations (appartenance à un groupe, chiffre d'affaires en croissance) et leurs valeurs sont sans effet. Le Tableau 1 reprend ces résultats. La Figure 8 récapitule les propositions suggérées par notre recherche, concernant les déterminants de l'engagement des organisa-

[10] Ces variables n'ayant pas un effet significatif sur la probabilité d'adopter une démarche de gouvernance de la sécurité de l'information, nous n'avons pas reporté les résultats correspondants dans le Tableau D1 de l'Annexe D.

tions dans la gouvernance de la sécurité de l'information.

3. DISCUSSION, CONTRIBUTIONS ET RECHERCHES FUTURES

3.1. Discussion des résultats

3.1.1. Processus d'engagement

Nous remarquons que les déterminants proposés du processus d'engagement des organisations dans la gouvernance de la sécurité de l'information sont très proches des quatre déterminants identifiés par Venkatesh *et al.* (2003) dans leur modèle unifié d'adoption et de diffusion des technologies (UTAUT pour *Unified Theory of Acceptance and Use of Technology*). En effet, ce modèle synthétise huit modèles antérieurs en quatre déterminants principaux : (1) la performance espérée de la démarche de gouvernance (valeur ajoutée, bénéfices, avantage concurrentiel) ; (2) l'effort déployé pour sa mise en œuvre (dépassement des freins, obstacles) ; (3) les conditions facilitatrices (connaissance d'organisations susceptibles d'aider l'organisation dans sa démarche) ; (4) l'influence sociale (normes subjectives, image, valeurs). La proximité de nos résultats avec ce modèle suggérerait que l'engagement des organisations dans le processus de gouvernance pourrait être comparé avec l'engagement dont les organisations pourraient faire état face à une innovation, en d'autres termes à l'adoption d'une innovation.

Plusieurs auteurs soulignent, en effet, dans leurs travaux que la gouvernance est une forme d'innovation. Par exemple Theys (2003), Bodet et Lamarche (2007) qualifient la gouvernance d'innovation institutionnelle ou organisationnelle. Dans le domaine des SI/TI, au travers d'un cahier de la revue *Management & Avenir* intitulé « Gouvernance et innovation à l'épreuve des technologies de l'information », Bidan et Trinquecoste (2010) mettent en exergue l'intérêt du tryptique « gouvernance – innovation – TI » pour les chercheurs en sciences de gestion. La sécurité a été assimilée à une innovation dans plusieurs travaux : par exemple, Kesh et Ratnasingam (2007) parlent d'une innovation exclusivement technique, tandis que Herath *et al.* (2010) évoquent une innovation technique et organisationnelle. De même, la perception des utilisateurs est régulièrement prise comme cadre d'analyse des innovations technologiques de sécurité (par exemple Charndra et Calderor, 2005 ; Cazier *et al.*, 2008). Il semblerait donc que la gouvernance de la sécurité de l'information puisse être appréhendée à la fois comme une innovation technique et organisationnelle.

Le modèle de Venkatesh *et al.* (2003), initialement adapté à l'évaluation des comportements individuels, a été étendu récemment par plusieurs auteurs au contexte organisationnel (par exemple, Curtis *et al.,* 2010 ; Gonzales *et al.,* 2011 ; Zhou, 2011). Il a ainsi permis de mesurer l'adoption d'un phénomène au niveau d'une organisation toute entière plutôt que de se focaliser sur l'intention d'utiliser au

niveau individuel. Nos contributions s'inscrivent dans cette perspective.

Cependant, toutes les conditions du modèle de Venkatesh *et al.* (2003) ne sont pas rassemblées dans notre enquête. En particulier, les quatre variables modératrices (genre, âge, expérience, utilisation volontaire) dont l'influence est significative dans le modèle, n'ont pas été prises en compte. Conscients de cette limite, nous pouvons conclure avec prudence sur la base de l'enquête menée que la théorie unifiée d'adoption de Venkatesh *et al.* (2003) peut être un modèle pertinent pour analyser le phénomène d'engagement dans la gouvernance de la sécurité de l'information.

3.1.2. Pratiques de gouvernance

Les réponses obtenues dans le cadre de notre enquête confirment que la gouvernance de la sécurité de l'information est un sous-ensemble à part entière de la gouvernance des SI/TI, puisque les organisations impliquées dans les deux démarches sont exactement les mêmes. Soulignons aussi que la responsabilité de la gouvernance de la sécurité est attribuée, selon les organisations, à des acteurs variés allant du responsable SI/TI (DSI), *risk manager*, responsable qualité/conformité, RSSI ou *security officer*, au directeur général. Au sein de l'échantillon étudié, le rattachement de la gouvernance à la DSI concerne plutôt les organisations faiblement ou moyennement exposées aux risques liés à l'information, où la fonction sécurité a une vocation plus opérationnelle que stratégique et managériale. Le rattachement de la gouvernance au management des risques, à l'audit ou au contrôle interne est plutôt typique des organisations exposées aux risques liés à l'information (secteurs d'activités tertiaires et quaternaires). Le rattachement de la gouvernance à la direction générale de l'organisation est privilégié lorsque l'information est le produit de l'organisation, et que le risque de l'organisation et celui lié à l'information sont quasi-confondus. Ces observations vont dans le sens de Bennasar *et al.* (2007), mais doivent être relativisées car elles dépendent fortement des structures organisationnelles en place et des secteurs d'activités. Il est intéressant aussi de relever un autre résultat de l'enquête : 29% des organisations interrogées pratiquant la gouvernance de la sécurité n'ont valorisé cette démarche ni en interne, ni vers l'extérieur, et 34% d'entre elles n'ont pas du tout communiqué sur leurs engagements. Preuve que la gouvernance de la sécurité de l'information n'est pas encore forcément considérée comme un atout dans la communication de l'organisation avec ses diverses parties prenantes (ou que l'organisation se situe dans un secteur d'activités qui ne requiert pas de communication sur le sujet). Enfin, les résultats de l'enquête nous amènent à nous demander si un engagement important de l'organisation dans la démarche de gouvernance de la sécurité de l'information entraîne des mutations organisationnelles. Les données empiriques collectées montrent que soixante organisations (87%) font déjà état de mutations organisationnelles au niveau 2 de la typologie précédente ; elles sont 100% au niveau 3. Il semblerait donc que ces deux événements soient corrélés : plus l'engagement de

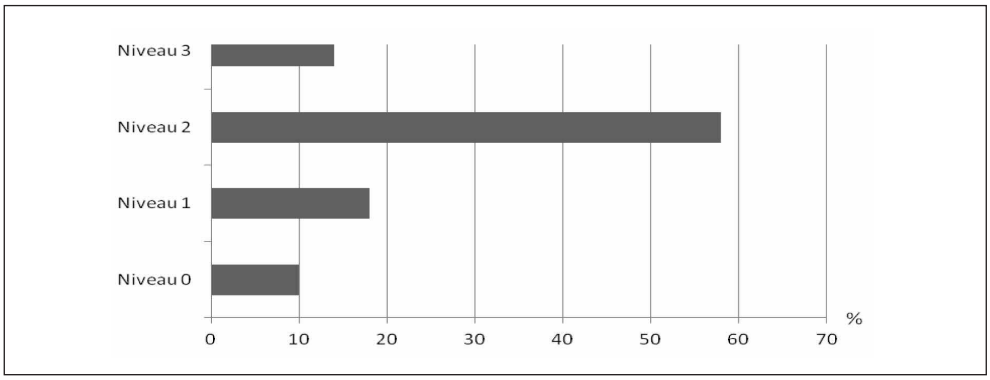
l'organisation dans la démarche de gouvernance de la sécurité de l'information est important, et plus les mutations organisationnelles engendrées le sont (il existe un lien d'alignement entre l'architecture organisationnelle et la sécurité de l'information).

Au vu des résultats de l'enquête, il nous a semblé intéressant de tester aussi si la perception des enjeux de la gouvernance de la sécurité de l'information était la même ou non, pour les organisations effectivement engagées dans la démarche et pour celles n'en ayant pas l'expérience pratique. Au regard de la distinction établie dans le questionnaire quant aux organisations engagées ou non dans la démarche de gouvernance de la sécurité de l'information, nous observons 100% de similitude dans le classement des trois premiers bénéfices en comparant les réponses de chaque type d'organisation ; le classement diffère ensuite de quelques organisations seulement (moins de dix) pour les bénéfices suivants. Concernant les obstacles perçus de la démarche, nous observons 100% de similitude sur tous les résultats du classement. Donc les enjeux stratégiques perçus de la gouvernance de la sécurité de l'information sont très similaires, que l'organisation soit engagée ou non dans cette démarche.

Pour finir, nous avons souhaité aborder la question de la maturité des organisations interrogées en matière de gouvernance de la sécurité de l'information : au regard de l'engagement ou non des organisations dans la démarche de gouvernance de la sécurité de l'information, nous pouvons compléter la typologie de l'IT Governance Institute (2006) et proposer une typologie de leur maturité en quatre niveaux :

- au niveau 0, nous situons les organisations qui ne pratiquent pas la gouvernance de la sécurité de l'information et jugent cette démarche peu utile voire inutile ; elles n'ont aucun projet en cours. Selon l'enquête menée, douze organisations (10%) se situent à ce niveau ;
- le niveau 1 regroupe les organisations qui ne pratiquent pas la gouvernance de la sécurité de l'information mais jugent tout de même la démarche positive (nécessaire ou indispensable) ; elles envisagent éventuellement des projets futurs. L'enquête montre que vingt-deux organisations (18%) se situent à ce niveau ;
- le niveau 2 est composé des organisations qui pratiquent la gouvernance de la sécurité de l'information et jugent cette démarche globalement intéressante (peu utile, nécessaire ou indispensable) ; elles ont un petit portefeuille de projets clôturés et/ou en cours, et leurs pratiques peuvent se traduire par des mutations internes. Soixante-neuf organisations (58%) se situent à ce niveau ;
- au niveau 3, nous classons les organisations qui pratiquent régulièrement la gouvernance de la sécurité de l'information et ont acquis une réelle expérience dans ces pratiques, qu'elles jugent indispensables ; leur portefeuille de projets comprend à la fois des projets clôturés, en cours et à venir, et leur engagement s'est traduit par des mutations organisationnelles. Dix-

Figure 9. Maturité des organisations sollicitées selon la typologie proposée



sept organisations (14%) se situent à ce niveau.

Ces informations sont illustrées par l'histogramme de la Figure 9.

L'âge et le niveau d'études du responsable de la sécurité n'influencent pas l'engagement de l'organisation dans la démarche de gouvernance de la sécurité de l'information.

3.2. Contributions théoriques, méthodologiques et pratiques

Du point de vue théorique, les résultats de notre enquête suggèrent que le modèle d'adoption unifié de Venkatesh *et al.* (2003) est un modèle pertinent d'analyse du processus d'engagement dans la gouvernance de la sécurité de l'information. L'enquête propose trois déterminants de l'engagement des organisations dans la gouvernance de la sécurité de l'information et renvoie une image fidèle des pratiques de gouvernance mises en œuvre par les organisations interrogées.

Sur le plan méthodologique, l'atout de notre recherche est certainement le taux de participation à l'enquête menée, soit 85,71%. Ce taux peut être apprécié au regard d'autres taux de participation obtenus lors de recherches empiriques comparables en sécurité de l'information, par exemple 1,6% pour Kotulic et Clark (2004) ; 8,77% pour Dagorn (2008) ; 1,57% pour Barlette (2009, 2011). Ces auteurs ont justifié leur faible taux de participation par divers arguments liés à la sensibilité et à la confidentialité du domaine : par exemple, Barlette (2011), citant Kotulic et Clark (2004), a souligné que peu d'organisations acceptent de parler de la sécurité car celle-ci constitue un sujet « envahissant » et « importun » ; les organisations ne souhaitent généralement pas traiter d'un sujet sensible à distance, et qui plus est, avec des personnes « extérieures »[11]. Ajoutons qu'au Luxembourg, les organisations sont ré-

[11] Kotulic et Clark (2004) constatent que, dans un domaine aussi sensible, des études à grande échelle ne sont pas adaptées car les organisations craignent de divulguer à une personne « extérieure » des informations relatives à la sécurité de leur SI. Ils conseillent de pratiquer plutôt des entretiens en face à face ou des études de cas, comme déjà mis en évidence par Eisenhardt (1989).

gulièrement interrogées dans le cadre d'enquêtes ayant un caractère obligatoire ; elles ne sont donc pas forcément disposées à répondre à des enquêtes non obligatoires. Le très bon taux de participation obtenu à notre enquête est le fruit de trois mois complets de sollicitations quotidiennes, et de mise en avant à la fois de nos connaissances académiques et de nos compétences professionnelles pour mériter la confiance des responsables interrogés dans un domaine où les recherches approfondies, les témoignages et les preuves sont rares (Siponen *et al.*, 2008).

Sur l'aspect pratique, cette recherche apporte aux managers des informations sur l'engagement des organisations dans la gouvernance de la sécurité de l'information et leurs pratiques de gouvernance. L'enquête suggère que la connaissance d'organisations engagées dans ou favorisant la démarche, la performance escomptée et l'effort déployé pour surmonter les difficultés ont une influence sur l'engagement des organisations dans la démarche. Elle décrit et actualise également les pratiques de quatre-vingt-six grandes entreprises engagées dans la gouvernance de la sécurité de l'information, sur les thèmes de la connaissance, des enjeux stratégiques, des conditions de mise en œuvre, de la maturité et de l'organisation de la gouvernance de la sécurité de l'information.

3.3. Limites et pistes de recherches futures

Sur le plan théorique, l'enquête menée ne nous permet pas de confirmer les déterminants suggérés par le modèle de Venkatesh *et al.* (2003) dont les résultats sont proches mais pas similaires. Il serait possible de vérifier l'applicabilité de la théorie unifiée d'adoption au processus d'engagement dans la gouvernance de la sécurité de l'information (et donc de tester si la gouvernance de la sécurité de l'information peut être assimilée à une innovation) en focalisant une prochaine enquête par questionnaire sur ces déterminants précis et tous leurs facteurs constitutifs.

Du point de vue empirique, la principale limite de notre enquête est certainement liée à l'échantillon : nous avons choisi de ne consulter que des grandes entreprises, alors que certaines PME, notamment celles pour lesquelles l'information est le cœur de métier, pratiquent peut-être la gouvernance de la sécurité de l'information ; le sondage d'un tel échantillon pourrait constituer une extension intéressante de la recherche.

CONCLUSION

Cet article propose une exploration des déterminants de l'engagement des organisations dans la gouvernance de la sécurité de l'information et de leurs pratiques en la matière. L'enquête conduite auprès de cent vingt organisations permet de formuler un modèle constitué de trois déterminants de l'engagement des organisations dans le processus de gouvernance de la sécurité de l'information : il suggère que la connaissance d'organisations engagées dans la gouvernance de la sécurité de l'information ou la promou-

vant, la performance espérée et l'effort déployé conditionnent l'engagement des organisations dans la démarche. Les réponses au questionnaire apprennent également à mieux connaître les pratiques actuelles de gouvernance de la sécurité de l'information mises en œuvre par les organisations.

Outre leur utilité pour les managers désireux de mieux connaître ou de mettre en place une démarche de gouvernance de la sécurité de l'information au sein de leur organisation, les résultats mis en avant par cette recherche peuvent également avoir une incidence sur les politiques publiques et institutions visant à faciliter la mise en œuvre de la gouvernance de la sécurité de l'information : en effet, au vu des faiblesses identifiées, cette dernière devrait passer par une promotion de la démarche en priorité auprès des grandes entreprises dont l'effectif est inférieur à mille salariés, et des grandes entreprises appartenant aux secteurs les moins favorables à la gouvernance de la sécurité de l'information (transports et télécommunications). Cette promotion pourrait être réalisée *via* des réseaux communautaires au sein desquels les organisations engagées dans la gouvernance exposeraient les grandes lignes de leur démarche et surtout des projets concrets mis en œuvre. Ces communautés de pratiques présenteraient l'intérêt de partager des connaissances (Hildreth & Kimble, 2002) ; idéalement, elles pourraient même se fixer des objectifs spécifiques à atteindre et ainsi prendre la forme de communautés stratégiques (Storck & Hill, 2000).

RÉFÉRENCES

Archibugi, D. & Michie, J. (1994), "Technology and Innovation: An Introduction", *Cambridge Journal of Economics*, Vol. 19, n° 1, p. 1-4.

Barlette, Y. (2009), « Vers une implication et une action des dirigeants de PME dans la sécurité de leur SI », *14e Congrès de l'Association Information et Management (AIM 2009),* Marrakech, Maroc, 10-12 juin.

Barlette, Y. (2011), « L'implication et l'action des dirigeants de PME dans la sécurité de leur Système d'Information », *16e Congrès de l'Association Information et Management (AIM 2011)*, La Réunion, 25-27 mai.

Bartlett, C.A. & Ghoshal, S. (1991), *Le Management sans frontières*, Editions d'Organisation, Paris.

Bennasar, M., Champenois, A., Arnould, P., Rivat, T. & Ballenghien, Y. (2007), *Manager la sécurité du SI: Planifier, déployer, contrôler, améliorer*, Dunod, Paris.

Bidan, M. & Trinquecoste, J.-F. (2010), « Gouvernance et innovation à l'épreuve des technologies de l'information », *Management & Avenir*, Vol. 4, n° 34, p. 125-127.

Bodet, C. & Lamarche, T. (2007), « La responsabilité sociale des entreprises comme innovation institutionnelle. Une lecture régulationniste », *Revue de la régulation*, n° 1, juin.

Boulet, P. (2007), *Management de la sécurité du SI*, Hermès Science Publications, Cachan.

Brotby, K. (2009), *Information Security Governance*, Wiley-Blackwell, Hoboken, New Jersey.

Carpentier, J.-F. (2009), *La sécurité informatique dans la petite entreprise – Etat*

de l'art et bonnes pratiques, Editions ENI, Saint-Herblain.

Cazier, J.A., Jensen, A.S. & Dave, D.S. (2008), "The Impact of Consumer Perceptions of Information Privacy and Security Risks on the Adoption of Residual RFID Technologies", *Communications of the AIS*, n° 23, p. 235-256.

Charndra, A. & Calderor, T. (2005), "Challenges and Constraints to the Diffusion of Biometrics in Information Systems", *Communications of the ACM*, Vol. 48, n° 12, p. 101-106.

Clusif (2010), « Menaces Informatiques et Pratiques de Sécurité en France », rapport, *http://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2010.pdf*.

Cohen, F. (2006), *IT Security Governance Guidebook With Security Program Metrics*, Auerbach Publishers Inc., Pennsauken, New Jersey.

Curtis, L., Edwards, C., Fraser, K.L., Gudelsky, S., Holmquist, J., Thornton, K. & Sweetser, K.D. (2010), "Adoption of Social Media for Public Relations by Nonprofit Organizations", *Public Relations Review*, Vol. 36, n° 1, p. 90-92.

Dagorn, N. (2008), « Politiques en matière de sécurité des systèmes d'information inter-organisationnels : une enquête dans dix grandes entreprises », *Systèmes d'Information et Management*, Vol. 13, n° 2, p. 97-125.

Davenport, T. (2002), « Privilégier l'information sur la technologie », http://www.lesechos.fr/formations/manag_info/articles/article_1_1.htm.

Davidson, R. & MacKinnon, J.G. (1984), "Convenient Tests for Logit and Probit Models", *Journal of Econometrics*, Vol. 25, p. 241-262.

Dhillon, G. & Backhouse, J. (2001), "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives", *Information Systems Journal*, n° 11, p. 127-153.

Dhillon, G., Tejay, G. & Hong, W. (2007), "Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations", *40th Hawaii International Conference on System Sciences*.

Dlamini, M.T., Eloff, J.H.P. & Eloff, M.M. (2009), "Information Security: The Moving Target", *Computers & Security*, n° 28, p. 189-198.

Eisenhardt, K.M. (1989), "Building Theories from Case Study Research", *Academy of Management Review*, Vol. 14, n° 532, p. 57-74.

Fernandez-Toro, A. (2009), *Management de la sécurité de l'information : Implémentation ISO 27001 - Mise en place d'un SMSI et audit de certification*, Eyrolles, Paris, 2e édition.

Gonzalez, G., Sharma, P.N. & Galletta, D. (2011), "The Antecedents of Internal Auditors' Adoption of Continuous Auditing Technology: Exploring UTAUT in an Organizational Context", *7th University of Waterloo Research Symposium on Information Integrity and Information Systems Assurance*, Toronto, Canada.

Goodhue, D.L. & Straub, D.W. (1991), "Security Concerns of Systems Users: A Study of Perceptions of the Adequacy of Security Measures", *Information and Management*, Vol. 20, n° 1, p. 13-27.

Gupta, A. & Hammond, R. (2005), "Information Systems Security Issues and Decisions for Small Businesses: An Empirical Examination", *Information Management and Computer Security*, Vol. 13, n° 4, p. 297-310.

Herath, T., Herath, H. & Bremser, W.G. (2010), "Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Man-

agement", *Information Systems Management*, Vol. 27, n° 1, p. 72-81.

Hildreth, P. & Kimble, C. (2002), "The Duality of Knowledge", *Information Research*, Vol. 8, n° 1, p. 1-27, http://informationr.net/ir/8-1/paper142.html.

IT Governance Institute (2006), *Information Security Governance: Guidance for Boards of Directors and Executive Management*, IT Governance Publishing, Cambridgeshire, 2e édition.

Johnston, A.C. & Hale, R. (2009), "Improved Security through Information Security Governance", *Communications of the ACM*, Vol. 52, n° 1, p. 126-129.

Kesh, S. & Ratnasingam, P. (2007), "A Knowledge Architecture for IT Security", *Communications of the ACM*, Vol. 50, n° 7, p. 103-108.

Klai, A. (2010), "Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies", *MIPRO 2010*, May 24-28, Opatija, Croatia, p. 1203-1208.

Knapp, K.J., Marshall, T.E., Rainer, R.K. & Ford, F.N. (2006), "Information Security: Management's Effect on Culture and Policy", *Information Management and Computer Security*, Vol. 14, n° 16, p. 24-36.

Knapp, K.J., Morris, R.F., Marshall, T.E. & Byrd, T.A. (2009), "Information Security Policy: An Organizational-Level Process Model", *Computers & Security*, n° 28, p. 493-508.

Kotulic, A. & Clark, J.G. (2004), "Why there aren't more Information Security Research Studies", *Information and Management*, Vol. 41, n° 5, p. 597-607.

Kraemer, S., Carayon, P. & Clem, J. (2009), "Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities", *Computers & Security*, n° 28, p. 509-552.

Krjukovs, D. & Strauss, R. (2009), "Information Security Governance as as Key Performance Indicator for Financial Institutions", *Computer Sciences*, n° 38, January, p. 161-167.

Markus, M.L. (1983), "Power, Politics, and MIS Implementation", *Communications of the ACM*, Vol. 26, n° 6, p. 430-444.

Martin, L. & Poussing, N. (2007), « Adoption et usages des Technologies de l'Information et de la Communication dans les entreprises de la branche des activités financières », CEPS/Instead, Economie et Entreprises, n° 08.

Martin, L. & Poussing, N. (2008a), « Les déterminants de l'adoption électronique par les entreprises: une analyse empirique sur données luxembourgeoises », CEPS/Instead, Enterprises Working Papers, n° 2008-03.

Martin, L. & Poussing, N. (2008b), "The Make-or-Buy Decision in ICT Services: Evidence from Luxembourg", CEPS/Instead, Enterprises Working Papers, n° 2008-06

Mitchell, R.C., Marcella, R. & Baxter, G. (1999), "Corporate Information Security Management", *New Library World*, Vol. 100, n° 1150, p. 213-227.

Monnoyer, M.C. (2003), « Le dirigeant confronté à la decision d'investissement en TIC », in *TIC et PME : des usages aux stratégies*, M. Boutary (Ed), L'Harmattan, Paris.

Morimune, K. (1979), "Comparisons of Normal and Logistic Models in the Bivariate Dichitomous Analysis", *Econometrica*, Vol. 47, p. 957-975.

Moulton, R. & Coles, R.S. (2003), "Applying Information Security Governance", *Computers & Security*, Vol. 22, n° 7, p. 580-584.

Pougnet-Rozan, S. (2005), « Entre mirage conceptuel et réalités managériales : quand des exigences de performance économique conduisent à des pratiques de responsabilité sociale… ou vice versa ? », *16e Congrès de l'Association francophone de Gestion des Ressources Humaines (AGRH 2005),* Paris Dauphine, 15-16 septembre.

Reix, R. (2004), *Systèmes d'information et management des organizations*, Vuibert, Paris, 5e édition.

Rockart, J.F. & Crescenzi, A.D. (1984), "Engaging Top Management in Information Technology", *Sloan Management Review*, Vol. 25, n° 4, p. 3-16.

Sapir, J. (2005), *Quelle économie pour le XXIe siècle?*, Odile Jacob, Paris.

Schou, C. & Schoemaker, D.P. (2006), *Information Assurance for the Enterprise: A Roadmap to Information Security*, McGraw Hill, New York.

Shi-Ming, H., Chia-Ling, L. & Ai-Chin, K. (2006), "Balancing Performance Measures for Information Security Management", *Industrial Management & Data Systems*, Vol. 106, n° 2, p. 242-255.

Siponen, M.T.A., Willison, R. & Baskerville, R. (2008), Power and Practice in Information Systems Security Research, *29th International Conference on Information Systems (ICIS 2008),* Paris, p. 13-21.

Storck, J. & Hill, P.A. (2000), "Knowledge Diffusion Through ²Strategic Communities²", in *Knowledge and Communities*, E.L. Lesser, M.A. Fontaine and J.A. Sulsher (Eds), Butterworth Heinemann, Oxford, p. 63-74.

Straub, D.W. & Welke, R.J. (1998), "Coping with Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly*, Vol. 22, n° 4, p. 441-469.

Teufel, S. (2003), "Information Security Management: State of the Art and Future Trends", *Information Security South Africa Conference (ISSA 2003),* Johannesburg, South Africa, July.

Theys, J. (2003), « La Gouvernance, entre innovation et impuissance : le cas de l'environnement », *Développement durable et territoires*, Dossier n° 2 : Gouvernance locale et développement durable, http://developpementdurable.revues.org/index1523.html.

Venkatesh, V., Morris, G.M., Davis, B.G. & Davis, D.F. (2003), "User Acceptance of Information Technology: Toward a Unified View", *MIS Quarterly*, Vol. 27, n° 3, p. 425-478.

Waddock, S.A. & Graves, S.B. (1997), "Corporate Social Performance-Financial Performance link", *Strategic Management Journal*, Vol. 18, n° 4, p. 303-319.

Williams, P. (2001), "Information Security Governance", *Information Security Technical Report*, Vol. 6, n° 3, p. 60-70.

Williams, P. (2007), "Executive and Board Roles in Information Security", *Network Security*, n° 8, p. 11-14.

Zhou, T. (2011), "Understanding Mobile Internet Continuance Usage from the Perspectives of UTAUT and Flow", *Information Development*, Vol. 27, n° 3, p. 207-218.

Annexe A

Tableau A1. Statistique descriptive des informations disponibles (% d'organisations)

Variables	**%**
Secteur d'activité	
Industrie	19.17
Construction	11.67
Transport	7.50
Télécommunications	2.50
Finance	21.67
Services	30.83
Commerce	6.67
Appartient à un groupe	72.50
Evolue sur le marché mondial	67.50
Le chiffre d'affaires a augmenté durant les 3 dernières années	49.17
Le chiffre d'affaires est resté stable durant les 3 dernières années	36.67
Le chiffre d'affaires a diminué durant les 3 dernières années	4.17
Types d'organisations connues engagées dans la gouvernance de la sécurité de l'information	
Client	34.17
Fournisseur	59.17
Concurrent	40.83
Autres organisations implantées au Luxembourg	61.67
Autres organisations implantées à l'étranger	57.50
Connaît un organisme de promotion de la gouvernance de la sécurité de l'information	56.67
Bénéfices retirés d'une démarche de gouvernance de la sécurité de l'information	
Améliorer l'image de l'organisation	29.17
Attirer de nouveaux clients/salariés	9.17
Se différencier de la concurrence	11.67
Instaurer la confiance	30.83
Etre en conformité avec la législation	32.50
Obtenir une certification	15.83
Améliorer les procédures de sécurité	51.67
Garantir les décisions et les activités à risque	25.83
Garantir la maîtrise de l'outil informatique	23.33
Augmenter la valeur de l'organisation	7.50
Accroître la prévisibilité et réduire l'incertitude des opérations de gestion	20.00
Ne pas engager sa responsabilité civile/légale	29.17
Optimiser les ressources de sécurité	20.83
Obstacles liés à la mise en œuvre d'une démarche de gouvernance de la sécurité de l'information	
Coût de la mise en œuvre	16.67
Manque de temps	20.83
Manque de ressources en interne	20.00
Manque de compétences en interne	11.67
Difficulté à trouver de l'information pertinente	5.83
Résistance au changement	15.00
Faible intérêt de la Direction	16.67
Traduction du concept en actions concrètes	8.33
Domaines prioritaires d'engagement dans une démarche de gouvernance de la sécurité de l'information	
Choix technologiques liés à la sécurité	28.33
Alignement de la sécurité de l'information sur la stratégie de l'organisation	44.17
Management du risque et réduction des impacts potentiels à un niveau acceptable	49.17
Management des ressources informationnelles	11.67
Evaluation de la performance par le suivi d'indicateurs de sécurité	15.83
Création de valeur par l'optimisation des investissements de sécurité	10.00

Annexe B

Tableau B1. Liste des variables introduites dans nos modèles

Nom de la variable	Label
INDUS	Appartenir au secteur de l'industrie
SERV	Appartenir aux autres secteurs
GROUP	Appartenir à un groupe
CHIDA	Avoir un chiffre d'affaires en croissance durant les trois dernières années
RESEAU10	Connaître des clients, des fournisseurs, des concurrents engagés dans la gouvernance de la sécurité de l'information
RESEAU11	Connaître d'autres organisations, implantées au Luxembourg ou à l'étranger, engagées dans la gouvernance de la sécurité de l'information
RESEAU20	Connaître des clients ou des fournisseurs engagés dans la gouvernance de la sécurité de l'information
RESEAU21	Connaître des concurrents engagés dans la gouvernance de la sécurité de l'information
RESEAU22	Connaître d'autres organisations, implantées au Luxembourg ou à l'étranger, engagées dans la gouvernance de la sécurité de l'information
ORGANISME	Connaître un organisme de promotion de la gouvernance de la sécurité de l'information
NB_BENEF	Nombre de bénéfices retirés d'une démarche de gouvernance de la sécurité de l'information
IMAGE	Améliorer l'image de l'organisation
ATTIRER	Attirer de nouveaux clients/salariés
DIFFERENCIER	Se différencier de la concurrence
INSTAURER	Instaurer la confiance
CONFORME	Etre en conformité avec la législation
CERTIFICATION	Obtenir une certification
AMELIORER	Améliorer les procédures de sécurité
GARANTIR	Garantir les décisions et les activités à risque
MAITRISE	Garantir la maîtrise de l'outil informatique
VALEUR	Augmenter la valeur de l'organisation
ACCROITRE	Accroître la prévisibilité et la réduire l'incertitude des opérations de gestion
RESPONSABILITE	Ne pas engager sa responsabilité civile/légale
RESSOURCE	Optimiser les ressources de sécurité
NB_OBST	Nombre d'obstacles liés à la mise en œuvre d'une démarche de gouvernance de la sécurité de l'information
COUT	Coût de la mise en œuvre
TEMPS	Manque de temps
PASRESSOURCE	Manque de ressources en interne
COMPETENCE	Manque de compétences en interne
INFORMATION	Difficulté à trouver de l'information pertinente
CHANGEMENT	Résistance au changement
DIRECTION	Faible intérêt de la Direction
ACTIONS	Traduction du concept en actions concrètes
NB_VAL	Nombre de domaines prioritaires d'engagement dans une démarche de gouvernance de la sécurité de l'information
TECHNO	Choix technologiques liés à la sécurité
ALIGNE	Alignement de la sécurité de l'information sur la stratégie de l'organisation
RISQUE	Management du risque et réduction des impacts potentiels à un niveau acceptable
RESSOURCE	Management des ressources informationnelles
PERF	Evaluation de la performance par le suivi d'indicateurs de sécurité
CREAVAL	Création de valeur par l'optimisation des investissements de sécurité

Annexe C

Tableau C1. Matrice SWOT des enjeux stratégiques de la gouvernance de la sécurité

	Bénéfices	Obstacles
Internes	- Amélioration des procédures de sécurité (management des risques, réponse aux incidents, etc.) (88%) - Optimisation des ressources de sécurité (72%) - Protection des responsabilités civile et légale (69%) - Assurance pour les décisions et activités critiques (68%) - Garantie sur la maîtrise des outils informatiques (par exemple, à l'égard des assureurs) (63%) - Accroissement de la prévisibilité et réduction de l'incertitude des opérations de gestion (547%) - Attraction de nouveaux salariés et clients (45%)	- Manque de temps (76%) - Manque de ressources internes (73%) - Coût de la mise en œuvre (72%) - Manque de compétences internes (53%) - Résistance au changement (49%) - Faible intérêt de la direction (43%)
Externes	- Gage de confiance pour les partenariats (79%) - Amélioration de l'image de l'organisation (73%) - Conformité avec la législation (ISO 27000, etc.) (66%) - Obtention de certifications ou labels qualité (58%) - Différenciation de la concurrence (43%) - Augmentation de la valeur de l'organisation (par exemple, actions sur les marchés financiers) (37%)	- Traduction du concept en actions concrètes (46%) - Difficulté à trouver de l'information pertinente, des supports, des conseils, de l'assistance pour la mise en œuvre (30%)

Annexe D

Tableau D1. Les déterminants de l'adoption de la gouvernance de la sécurité de l'information (modèle Logit)

Nom variable	Modèle 1	Modèle 2	Modèle 3	Modèle 4	Modèle 5	Modèle 6	Modèle 7
Constante	-0.7332	-1.0428	-0.8604	-0.8936	**-1.3922***	**-1.2516***	-0.6166
	(0.6815)	(0.6687)	(0.6637)	(0.6775)	**(0.7171)**	**(0.7070)**	(0.6223)
INDUS	-0.8245	-0.8839	-0.8768	-0.9478	**-0.9940***	-0.7896	**-1.4005*****
	(0.5411)	(0.5446)	(0.5410)	(0.5540)	**(0.5623)**	(0.5696)	**(0.5329)**
SERV	Référence	Référence	Référence	Référence	Référence	Référence	Référence
GROUP	0.4075	0.5157	0.3749	0.4738	0.6158	0.4200	**1.0921***
	(0.5893)	(0.5852)	(0.5796)	(0.5905)	(0.6138)	(0.6114)	**(0.5712)**
CHIDA	0.1612	0.2075	0.2388	0.2441	0.1885	0.3058	-0.0932
	(0.5090)	(0.5149)	(0.5137)	(0.5223)	(0.5334)	(0.5337)	(0.4934)
NB_RESEAU	**0.5903*****	**0.6055*****	**0.5966*****	**0.5921*****	X	X	X
	(0.1617)	**(0.1667)**	**(0.1617)**	**(0.1678)**			
RESEAU10	**X**	**X**	**X**	X	**1.4350*****	X	X
					(0.5486)		
RESEAU11	**X**	**X**	**X**	X	**1.1240****	X	X
					(0.5568)		
RESEAU20	**X**	**X**	**X**	X	X	0.7884	X
						(0.5750)	
RESEAU21	**X**	**X**	**X**	X	X	**1.2089***	X
						(0.7050)	
RESEAU22	**X**	**X**	**X**	X	X	**1.0726***	X
						(0.5573)	
ORGANISME	**X**	**X**	**X**	X	X	X	**1.6535*****
							(0.5339)
NB_BENEF	**0.2937****	**0.2682****	**0.3523****	**0.3036****	**0.2694****	**0.2670****	**0.3371*****
	(0.1268)	**(0.1263)**	**(0.1388)**	**(0.1378)**	**(0.1290)**	**(0.1286)**	**(0.1257)**
NB_OBST	-0.2700	X	X	X	X	X	X
	(0.1821)						
DIRECTION	X	X	**-1.1713***	-1.0030	X	X	X
			(0.6743)	(0.6902)			
ACTIONS	X	**-1.8703****	X	**-1.7077***	**-2.0544****	**-2.0409****	**-2.2397****
		(0.9421)		**(0.9912)**	**(0.9710)**	**(1.0039)**	**(1.0150)**
NB_VAL	0.0185	0.1125	-0.0546	0.1223	0.1579	0.1362	-0.0224
	(0.2272)	(0.2432)	(0.2167)	(0.2484)	(0.2494)	(0.2477)	(0.2403)
Nombre d'observations	120	120	120	120	120	120	120
% concordance	85.2	85.5	85.3	86.3	85.6	85.9	81.7
-2 Log L	100.322	98.585	99.514	96.444	97.059	96.267	103.883

* significatif au seuil de 10%, ** significatif au seuil de 5%, *** significatif au seuil de 1%
Coefficient, écart type entre parenthèses.

François de CORBIÈRE est maître de conférences en sciences de Gestion à l'Ecole des Mines de Nantes. Membre du LEMNA, ses recherches portent principalement sur les systèmes d'information interorganisationnels. Il travaille plus particulièrement sur les concepts d'intégration et de synchronisation à travers l'analyse de la coordination des échanges et de ses effets, tant sur les transformations organisationnelles que sur la qualité des données.

Adresse : Ecole des Mines de Nantes, Dpt Sciences Sociales et de Gestion, 4 rue Alfred Kastler, 44307 NANTES.

Mail : francois.de-corbiere@mines-nantes.fr

Nathalie DAGORN est Professeur Assistant à ICN Business School Nancy-Metz, membre du laboratoire CEREFIGE. Titulaire d'un doctorat en sciences de gestion obtenu à l'Université de Nancy 2, ses thématiques de recherche concernent principalement le management de la sécurité de l'information et la coopération des systèmes d'information dans les entreprises.

Adresse : ICN Business School Metz, 3 Place Edouard Branly, 57070 Metz

Mail : nathalie.dagorn@icn-groupe.fr

Aurélie DUDEZERT est Maître de Conférences en Sciences de Gestion Habilitée à Diriger les Recherches à l'Ecole Centrale Paris. Spécialiste du Management des Connaissances elle est aujourd'hui en charge du développement de l'équipe en Sciences Economiques et Sciences de Gestion de l'Ecole Centrale Paris (Equipe de recherche sur les Politiques de Croissance fondées sur la Connaissance-EPOCC) qui se donne pour objectif d'étudier les nouveaux modèles de croissance de l'économie et les nouveaux modes d'organisation des entreprises à l'heure de l'Economie de la Connaissance.

Adresse : Laboratoire Génie Industriel, Ecole Centrale Paris, Grande Voie des Vignes, 92295 Châtenay-Malabry

Mail : aurelie.dudezert@ecp.fr

Myriam KAROUI est doctorante à l'Ecole Centrale Paris dans le domaine du Management des Systèmes d'Information. Au sein de l'équipe EPOCC (Equipe de recherche sur les Politiques de Croissance fondées sur la Connaissance), ses recherches portent sur les médias sociaux, les outils des réseaux sociaux et leur appropriation ainsi que les nouvelles pratiques de travail nées avec l'émergence des outils 2.0.

Adresse : Laboratoire Génie Industriel, Ecole Centrale Paris, Grande Voie des Vignes, 92295 Châtenay-Malabry

Mail : myriam.karoui@ecp.fr

Olivier MEIER est Maître de conférences des Universités, habilité à Diriger des Recherches en sciences de Gestion. Membre de l'Institut de Recherche en Gestion (UP EC), ses thèmes de recherche portent sur les stratégies de croissance (fusions-acquisitions, alliances stratégiques, réseaux d'entreprises), la gestion de l'innovation et le management du changement.

Adresse : Institut de recherche en gestion, Universite paris est, Avenue pierre point, 77 127 Lieusaint

Mail : olmeier@yahoo.fr

Audrey MISSONIER est professeur au sein du Groupe Sup de Co Montpellier et membre du laboratoire MRM (Montpellier Recherche en Management). Elle concentre ses recherches, notamment, sur les processus d'innovation technologique dans le cadre de fusions et d'alliances stratégiques, et sur l'étude de la dynamique de changement.

Adresse : Groupe Sup de Co Montpellier Business School, 2300 avenue des Moulins, 34185 Montpellier

Mail : A.Missonier@supco-montpellier.fr

Stéphanie MISSONIER est professeur assistante en PTC à HEC Lausanne, et membre du laboratoire GREDEG (Groupe de Recherche en Science de Gestion) de Nice-Sophia Antipolis. Ses domaines de recherche concernent tout particulièrement

les problématiques relatives à l'échec des projets de Technologie de l'Information.

Adresse : Université de Lausanne, Faculté des HEC, Quartier Unil Dorigny, Bâtiment Internef, 1015 Lausanne, Suisse

Mail : stephanie.missonier@unil.ch

Nicolas POUSSING est chercheur, responsable de l'Axe « Organisation industrielle et société de la connaissance » au CEPS / INSTEAD, un établissement public de recherche situé au Luxembourg. Il est chercheur associé au laboratoire CREM de Rennes. Titulaire d'un doctorat en économie de l'Université de Nancy 2, ses intérêts de recherche se focalisent sur la responsabilité sociale des entreprises (adoption et relation de la RSE avec l'innovation). Il analyse aussi les effets des usages d'Internet (effet sur le capital social, sur le bonheur…).

Adresse : CEPS/INSTEAD, 3 Avenue de la Fonte, L-4364 Esch-sur-Alzette

Mail : nicolas.poussing@ceps.lu

Frantz ROWE est Professeur en sciences de Gestion à l'Université de Nantes. Membre du LEMNA et chercheur à SKEMA Business School, ses recherches portent principalement sur les effets transformationnels des systèmes d'information sur les organisations. Il s'intéresse notamment aux systèmes inter-organisationnels, aux centres d'appels et aux systèmes intégrés tels que PLM.

Adresse : Institut d'Economie et Management de Nantes, Chemin de la Censive du Tertre, 44322 Nantes

Mail : frantz.rowe@univ-nantes.fr

François-Charles WOLFF est professeur en Sciences Economiques à l'Université de Nantes où il dirige le Laboratoire d'Economie et de Management de Nantes Atlantique. Il est également chercheur associé à l'Institut National des Etudes Démographiques. Il a écrit, seul ou en collaboration, deux ouvrages et plus de 80 articles dans des revues à comité de lecture nationales et internationales dans des champs variés couvrant notamment l'économie de la famille, l'éducation, les migrations, la santé, l'économie du travail, le transport ou bien encore l'économie maritime.

Adresse : Institut d'Economie et Management de Nantes, Chemin de la Censive du Tertre, 44322 Nantes

Mail : francois.wolff@univ-nantes.fr