Implication et action des dirigeants : quelles pistes pour améliorer la sécurité de l'information en PME ?

Yves BARLETTE

Groupe Sup de Co, Montpellier Business School
Montpellier Research in Management

RÉSUMÉ

Cet article traite de la sécurité des systèmes d'information (SSI) des PME, qui ont des problèmes souvent plus importants en matière de SSI que les entreprises de plus grande taille. Il s'intéresse plus particulièrement aux dirigeants de PME, car de nombreux spécialistes et scientifiques s'accordent sur leur rôle majeur. Pourtant certains dirigeants ne s'impliquent pas ou n'agissent pas dans la SSI de leur entreprise, avec des conséquences potentiellement désastreuses pour leur activité. Souvent, implication et action sont confondues, ce qui limite la compréhension de cette problématique.

La question de recherche développée dans cette étude exploratoire est : Comment améliorer le rôle du dirigeant dans la SSI de sa PME ? *Pour traiter cette question, nous avons étudié (1) les facteurs conditionnant leur implication et leurs actions, (2) les conséquences de leur implication et de leurs actions, (3) comment les rôles sont partagés dans la gestion de la SSI.*

Une méthodologie qualitative et une approche interprétative ont été adoptées pour mener à bien cette étude empirique. Les résultats complètent et améliorent la compréhension des facteurs conditionnant l'implication et l'action des dirigeants de PME en matière de SSI. Quatre situations-types ont été identifiées, qui ont servi de cadre d'analyse des rôles des divers acteurs impliqués dans la SSI des PME. Les contributions théoriques sont d'une part la mise en évidence de nouveaux facteurs d'implication et d'action des dirigeants et d'autre part, comme la fonction de responsable du SI et a fortiori de responsable de la SSI s'avère très rare dans les plus petites PME, il a été identifié une prise en charge informelle par certains salariés de la SSI de leur PME. Certains facteurs expliquant cette prise en charge, ainsi que les problèmes rencontrés par ces salariés-RSSI ont été identifiés. Les apports managériaux correspondent aux possibilités de mieux impliquer le dirigeant de PME dans la SSI de son entreprise, mais la principale contribution reste la mise en évidence de l'importance capitale d'une meilleure gestion du salarié en charge de la SSI, notamment lorsque cette prise en charge est informelle. L'originalité de ce travail correspond à l'étude de manière dissociée de l'implication et l'action des dirigeants, qui a apporté une meilleure compréhension du partage des rôles en matière de SSI et qui a permis de proposer des recommandations pratiques d'amélioration de la SSI en fonction des situations identifiées.

Mots-clés : sécurité, dirigeant, implication, action.

ABSTRACT

This article focuses on the role of SME managers in IS security (ISS), as these companies often suffer from more important ISS problems than larger companies. Although many specialists and scholars agree on the importance of their role, SME managers sometimes show little involvement or little action regarding ISS, leading to potentially disastrous consequences. In the literature, involvement and action are often merged, which limits the exploration of this issue. The research question dealt with in this paper is: How to improve the role of managers in their company's ISS? *In order to respond, we examined (1) the barriers and drivers of managers' involvement and action, (2) the consequences of their involvement and actions (3) how the roles in ISS management are shared out. This empirical study uses a qualitative methodology and an interpretive approach. The results extend our understanding of the factors that influence managers' involvement and action in ISS. Four contexts were identified, which were used as a framework for the analysis of the roles of the various people involved in SME ISS. This paper makes a theoretical contribution by shedding light on new factors of managers' involvement and actions. The smallest SMEs seldom have a chief information officer (CIO) or a chief information security officer (CISO). In this case, we found that employees sometimes assume informal responsibility for IS and ISS. We identified various factors to explain this informal position and several related issues. We also contribute to managerial practices by identifying avenues to better involve managers in the ISS of their SMEs. Our major contribution is showing for the first time that when an employee assumes the role of a CISO, whether informally or not, it is of utmost importance to provide top management support. This study is original because managers' involvement and actions are studied separately, which provides more detailed results and allowed us to propose practical recommendations to improve ISS, according to the identified situations.*

Keywords: Security, manager, involvement, action.

INTRODUCTION

Cet article est consacré à la sécurité de l'information qui se définit par "*la protection de la confidentialité, intégrité, et disponibilité de l'information et de ses éléments critiques, incluant les logiciels et matériels qui utilisent, mémorisent, traitent et transmettent cette information au travers de l'application de principes, technologies, formations et sensibilisations*" (Khoo *et al.* 2010, p.49).

La littérature en Sciences de Gestion insiste depuis longtemps sur le fait que la SSI doive être considérée comme un problème de gestionnaires et non de techniciens (Davenport, 2002 ; Kayworth et Whitten, 2010 ; Reix, 2004). L'objectif de cet article est de resituer la problématique de la SSI dans une dimension organisationnelle, car des lacunes existent tant sur le plan de l'élaboration de théories (Coles-Kemp, 2009 ; Dhillon et Backhouse, 2001 ; Dlamini *et al.*, 2009), qu'en matière de recherches empiriques (Kotulic et Clark, 2004). De nombreux auteurs ont déclaré que la SSI devait être prise en compte au niveau de la direction générale de l'entreprise (Markus, 1983 ; Longeon et Archimbaud, 1999 ; Friend et Pagliari, 2000 ; Knapp *et al.*, 2006). Les dirigeants doivent donc être considérés comme le point de départ d'une mise en place d'une SSI qui puisse être considérée comme satisfaisante (Robinson et Volonino, 2004), ce qui rend leurs actions importantes.

L'implication du dirigeant est, elle aussi, considérée comme capitale dans la mise en place, le maintien et le succès d'actions relatives à la sécurité des S.I. (Johnston et Hale, 2009). Rockart et Crescenzi (1984) ont déclaré que les dirigeants doivent "*réaliser que l'information est une ressource stratégique... Et ressentir de manière accrue le besoin d'être informés, motivés, et engagés dans les SI*" (p2). Cette importance de l'implication et de l'action du dirigeant en matière de SSI a été mise en évidence non seulement dans la littérature, mais aussi dans de nombreux guides de bonnes pratiques, ou encore dans des normes dédiées à la SSI, telles les normes ISO 270xx[1].

Hoff (2008) a soulevé le fait que peu d'études ont cherché à comprendre en quoi consistait l'implication des dirigeants, d'autres auteurs ont relevé le même problème au sujet de leur participation et de leurs actions (Dong, 2008 ; Zwikael, 2008). Mais plus rares encore sont les travaux s'intéressant aux facteurs d'implication et/ou d'action des dirigeants, à l'incidence de cette implication et/ou actions et aux principales actions que doivent accomplir ces dirigeants (Loonam et McDonagh, 2005).

Cette étude portera sur la SSI dans les PME, car elles présentent de nombreux intérêts : un intérêt managérial tout d'abord, parce qu'en France, selon l'INSEE (2011) plus de 97% des entreprises de plus de 10 salariés comptent moins de 250 employés. Dans les enquêtes portant sur la SSI, ce sont aussi les PME qui obtiennent les plus mauvais résultats (Labodi et Michelberger, 2010). Deuxièmement, un intérêt scientifique, car peu de travaux ont traité de la sé-

[1] ISO 27001 et 27002 sont les plus connues de cette série qui s'étend à 32 normes, dont 16 étaient finalisées fin avril 2012 (http://www.iso27001security.com).

curité dans les PME (Kyobe, 2008), même si les PME font face à des problèmes plus importants que ceux rencontrés par de plus grandes entreprises : problèmes de recrutement de personnes qualifiées dans les TIC (Monnoyer, 2003 ; Pritchard, 2010), dans l'appréciation des risques encourus (Gupta et Hammond, 2005) et de lacunes en termes de sensibilisation à la SSI (Mitchell *et al.*, 1999 ; Rees, 2010). Les PME ne disposent ni des ressources matérielles et techniques (Labodi et Michelberger, 2010) ni des ressources humaines et financières (Lee et Larsen, 2009) pour gérer correctement leur SSI. Les dirigeants, s'ils peuvent être secondés par des responsables de la sécurité du S.I. (RSSI) ou au moins par leur responsable du S.I. (RSI) dans les plus grandes entreprises, se retrouvent de plus en plus seuls quand la taille de leur entreprise diminue. En conséquence, l'implication et les actions des dirigeants vont revêtir de plus en plus d'importance dans la SSI de leur entreprise.

La question de recherche développée dans cette étude exploratoire est : *Comment améliorer le rôle du dirigeant dans la SSI de sa PME ?* Pour traiter cette question, nous avons choisi de nous intéresser plus particulièrement à l'implication et à l'action des dirigeants et au partage des rôles dans la gestion de la SSI.

En première partie, l'analyse de la littérature a pour objectif d'apporter un éclairage sur l'implication et l'action des dirigeants en matière de SSI et la distinction qui peut être réalisée entre implication et action. Ceci amènera à traiter des facteurs qui peuvent renforcer ou non cette implication et cette action des dirigeants, et de l'éventuelle incidence de l'implication et de l'action des dirigeants sur la SSI de leur entreprise. Après une partie méthodologique, la troisième partie présente les résultats d'une étude empirique correspondant à 29 entretiens conduits auprès de huit PME appartenant à des secteurs variés, tels que la commercialisation de compléments alimentaires, la fabrication de peintures ou encore la conception et la vente de systèmes photovoltaïques. La quatrième partie correspond à la discussion de ces résultats et à la formulation de recommandations pratiques. La cinquième partie résume les apports de ce travail. La conclusion présente les limites de cette recherche ainsi que les pistes ouvertes pour de futurs travaux.

I. IMPLICATION ET ACTIONS DES DIRIGEANTS

L'implication et l'action, même si elles sont souvent traitées comme un seul construit dans la littérature en S.I., peuvent être considérées comme deux éléments différents (Barki et Hartwick, 1989; Jarvenpaa et Ives, 1991). Ainsi, les facteurs de l'implication du dirigeant vont d'abord être examinés, suivis par l'examen des facteurs relatifs à leur action. Enfin, les relations entre implication et action vont être étudiées.

I.1. L'implication des dirigeants

L'implication peut être définie comme un "*état subjectif psychologique*" (Barki et Hartwick, 1989, p. 59). Elle correspond aussi au degré de préoccupation du dirigeant et à l'importance perçue, relative au SI de son entreprise (Jarvenpaa et Ives, 1991 ; Stemberger *et al.*, 2011). Enfin, l'implication est aussi assimilable au sentiment que les ressources et le temps consacrés sont "sagement investis" (Sanders et Courtney, 1985, p. 93).

Cette implication ne se traduira pas forcément par des actions directes, qui seront traitées dans le paragraphe suivant, mais au moins par des actions indirectes (Jarvenpaa et Ives, 1991). Par actions indirectes, il sera par exemple question pour le dirigeant de la PME de mettre l'accent sur la sécurité de l'information lors de communications orales plus ou moins informelles (Jarvenpaa et Ives, 1991). Ces actions indirectes pourront aussi correspondre aux relations entre le dirigeant et les personnes en prise directe avec la SSI telles que la valorisation, des encouragements, la sélection de responsables, etc. (Ragu-Nathan *et al.*, 2004). De la même manière, certains impacts indirects du soutien de la direction seront le maintien d'un bon positionnement du personnel en charge du S.I. dans la hiérarchie de l'organisation (Stemberger *et al.*, 2011) ou encore la création d'un "contexte de soutien" dans l'organisation (Ragu-Nathan *et al.*, 2004). Le soutien de la direction est donc essentiel dans l'obtention d'une adhésion des employés à la SSI (Avolio, 2000 ; Johnston et Hale, 2009). L'implication pourra enfin influencer de manière favorable la perception par le dirigeant des propositions du personnel en charge du S.I. (Jarvenpaa et Ives, 1991).

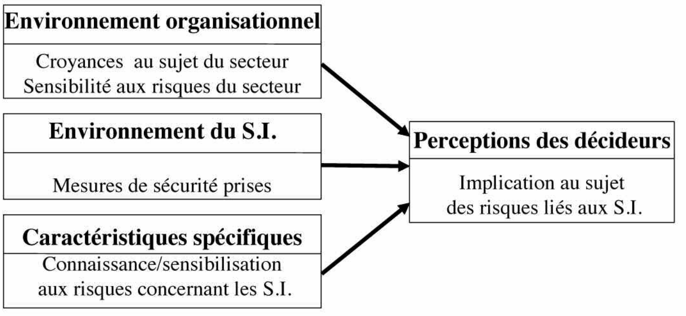
Très peu d'études se sont intéressées aux facteurs déterminants de l'implication des dirigeants. Dans le domaine des S.I, les travaux suivants ont été identifiés : Tout d'abord, le passé d'un dirigeant influe sur le degré de son implication dans le management des technologies de l'information. Il a été démontré que des éléments tels que le niveau d'éducation et l'expérience dans une fonction donnée (Song, 1982) ainsi que l'âge (Norburn et Birley, 1988), ont une incidence sur leur implication. Il a aussi été montré que l'ancienneté du dirigeant dans l'organisation (Helmich et Brown, 1972), son ancienneté dans sa position hiérarchique (Stevens *et al.*, 1978), façonnent leurs attitudes et leurs perceptions relatives aux opportunités et aux problèmes se présentant dans leur entreprise. Enfin, d'après Jarvenpaa et Ives (1991), l'implication du dirigeant est influencée par son expérience, l'environnement organisationnel, et la participation du dirigeant à la gestion du SI de son entreprise.

Dans le domaine de la SSI, Goodhue et Straub (1991) ont montré que la perception par les décideurs des risques en SI est anormalement basse comparée à celle de l'ensemble des risques que court leur entreprise ; ils ne sont donc pas correctement préparés à faire face aux risques relatifs aux SI. L'intérêt de leur modèle réside dans le fait qu'il se destine spécifiquement à la SSI ; aucune autre étude à notre connaissance n'a porté depuis vingt ans sur ce domaine précis.

Leur étude a déterminé que l'implication des décideurs dans la SSI de l'organisation est fonction de (figure 1) :

1. l'environnement organisationnel (risque inhérent au secteur) ;
2. l'étendue des efforts consentis pour contrôler ces risques ;

Figure 1. Modèle de l'implication des décideurs, d'après Goodhue et Straub (1991)



3. facteurs spécifiques, tels que la connaissance de sinistres précédents ou l'expérience en SI.

Ce modèle amalgame l'implication et les actions (mesures de sécurité prises), ce qui pourrait fausser l'estimation de l'implication : avant de pousser plus loin cette réflexion, il est nécessaire d'examiner la littérature concernant l'action des dirigeants.

I.2. Les actions des dirigeants

Dans cet article, les actions seront définies comme la participation et les interventions directes des dirigeants dans la gestion de la sécurité de leur S.I. (Jarvenpaa et Ives, 1991).

Par exemple, le dirigeant a-t-il décidé de mettre en place une nouvelle procédure de sécurité ? Est-ce lui qui appelle la société extérieure pour faire dépanner un salarié qui est bloqué ?

Dans un premier temps les intérêts de l'action des dirigeants vont être examinés, puis certains facteurs, favorisant ou limitant les actions, seront identifiés dans la littérature.

Une entreprise, *a fortiori* une PME, dispose de ressources limitées et, comme il est impossible d'obtenir une sécurité parfaite, la direction doit donc réaliser les arbitrages appropriés coûts/bénéfices et décider de manière rationnelle du niveau de risque qu'elle souhaite assumer (Dutta et McCrohan, 2002 ; Anderson et Choobineh, 2008). L'un des rôles clés de la direction est de définir l'équilibre désiré entre la mise en œuvre de la SSI et les pertes possibles en termes de productivité (Reid et Gilbert, 2009) en fonction de son métier et de son activité (Johnston et Hale, 2009). Seule la direction est en position de réaliser ce choix.

Mais les aspects stratégiques et financiers ne doivent pas être les seuls traités : il faut aussi faire évoluer l'entreprise elle-même, dans sa globalité, en incluant les aspects humains. Dutta et McCrohan (2002) soulignent le rôle de la direction dans l'adoption de caractéristiques organisationnelles désirables pour obtenir une sécurité satisfaisante. Hofstede *et al.* (1990) ont mis en évidence le fait que les valeurs des dirigeants deviennent les pratiques des membres des organisations. En effet, en vertu de son rôle, la direction est capable d'assurer une allocation suffisante des ressources et d'agir comme un agent du changement afin de créer un environnement favorable (Dong, 2008 ; Lucas, 1981 ; Kankanhalli *et al.*, 2003). De plus, le dirigeant dispose de l'autorité nécessaire pour influencer les autres membres de l'entreprise, il est ainsi plus susceptible de réussir à surmonter une résistance organisationnelle et des barrières culturelles (Markus, 1983 ; Dutta et McCrohan, 2002 ; Knapp *et al.*, 2006 ; Boss *et al.*, 2009).

Enfin, un support actif de la part des dirigeants transmet des signaux forts dans toute l'organisation (Grover, 1993). Des travaux scientifiques ont montré que le succès des projets en S.I. ainsi que l'implication et la propension à agir des salariés sont directement dépendants des actions concrètes du décideur (Dong *et al.*, 2009 ; Forcht et Ayers, 2000).

A l'inverse, une faible prise en charge de la SSI par les dirigeants est synonyme de salariés qui intègreront mal les bonnes pratiques et de procédures de sécurité insuffisamment appliquées (Knapp *et al.*, 2006). Ces derniers éléments font donc apparaître l'incidence du comportement des dirigeants sur celui des salariés, qui rend l'étude des dirigeants d'autant plus importante dans la recherche de facteurs d'amélioration de la SSI.

Le dirigeant peut alors mettre en place les procédures et les règlements nécessaires : selon Ashenden (2008), la personne en charge de la gestion de la SSI doit faire partie des dirigeants de l'entreprise car elle dispose des compétences entrepreneuriales nécessaires et pourra agir de manière proactive en tant qu'agent du changement. A partir de là, des guides de bonnes pratiques ou des normes de SSI[2] peuvent fournir une première approche de la gestion de la SSI et donner les bases d'une approche cohérente de la SSI (Vermeulen et Von Solms, 2002 ; Bruce et Dempsey, 1997).

Il appartient aux dirigeants de prendre en compte non seulement les aspects comportementaux et les procédures à respecter en matière de SSI (Boss *et al.*, 2009) mais aussi certains aspects technologiques (Jarvenpaa et Ives, 1991).

Pourtant, les dirigeants baissent parfois les bras car ils manquent souvent de connaissances en S.I. (Rainer *et al.*, 2007) alors que la sécurité organisationnelle ne doit pas être abandonnée à la fonction "technologie" ou "sécurité" de l'information (Ross et Weill, 2002 ; Williams, 2007).

Malgré l'importance de leur rôle, les dirigeants n'agissent pas forcément : par exemple, une étude de Gupta et Hammond (2005) a mis en évidence que les dirigeants de PME sont trop préoccupés par les opérations "au jour le jour" pour formuler et mettre en place une stratégie liée à la SSI de leur entreprise ; leur marge de manœuvre peut aussi être limitée par le budget. Les dirigeants manquent enfin de connaissances techniques et d'une réelle compréhension de ce que représente la SSI. Ceci nuit à leur prise en charge de la SSI, d'autant plus qu'ils sont peu compétents dans le

[2] Les auteurs font référence à BS7799-1, proche de ISO/IEC 27002 en 2012.

choix des technologies appropriées (Hagen *et al.*, 2008).

I.3. Les relations entre l'implication et l'action des dirigeants

Le cheminement classique et logique correspondrait à une implication conduisant à l'action et des actions renforçant l'implication, comme l'ont montré Goodhue et Straub (1991) ainsi que Jarvenpaa et Ives (1991). Barlette (2008) a aussi utilisé ce cadre d'analyse dans son étude.

Selon ces auteurs, deux situations peuvent se présenter : premièrement celle correspondant à un dirigeant peu impliqué et qui agit peu. On peut s'attendre à ce que cette situation, contraire à tout ce qui est démontré et conseillé dans ce domaine, ait des conséquences néfastes sur le niveau de SSI de l'entreprise. A l'opposé, la situation correspondant à un dirigeant impliqué et qui va agir devrait être la plus bénéfique pour la SSI de l'entreprise. Enfin, le modèle en figure 1 suggère un "cercle vertueux" de l'implication croissante d'un dirigeant, au fur et à mesure de ses actions.

Pourtant, certains dirigeants pourraient être forcés de se conformer à certaines exigences sectorielles et/ou réglementaires (Forte, 2008 ; Knapp *et al.*, 2009 ; Smith *et al.* ; 2010). On parlerait alors de "SSI obligatoire". En effet, il existe de nombreuses réglementations ayant des rapports avec la SSI : une des plus connues est la loi informatique et libertés (CNIL) qui va engager la responsabilité pénale du dirigeant afin d'éviter que les informations nominatives gérées par l'entreprise soient "*déformées, endommagées ou communiquées à des tiers non autorisés*". Certaines réglementations vont dépendre du secteur d'activité de l'entreprise (banque, santé…), d'autres dépendront de la taille, du statut ou de l'activité de l'entreprise (loi sur la Sécurité Financière, Bâle II, Sarbanes Oxley…).

D'autre part, la SSI en elle-même présente des intérêts qui vont au-delà de la seule protection des informations. Le concept de ROSI ou Return On Security Investment (Clusif, 2004 ; Drugescu et Etges, 2008) met en avant des arguments technologiques (réduction des coûts d'infrastructures et des incidents de sécurité et nuisances), métiers (diminution des primes d'assurance, amélioration de l'image et de la qualité de service), réglementaires (responsabilités civiles, pénales, liées à l'activité ou au secteur d'activité) et normatifs (pressions du marché pour adopter des normes telles ISO 27000 par exemple).

Johnston et Hale (2009) ont montré que les deux premiers facteurs de prise en charge de la SSI par les dirigeants sont la nécessité de conformité avec les responsabilités civiles et pénales, suivie par l'amélioration de l'image de l'entreprise. Dans le cadre d'un fonctionnement en sous-traitance ou d'un accord de partenariat, certaines entreprises doivent parfois adopter des normes ou méthodes de sécurité : ces entreprises sont sujettes à plus de contrôles et sont parfois soumises à des audits complets (Pritchard, 2010). Enfin, prouver que l'on est en conformité avec certaines normes ou méthodes peut aider à négocier à la baisse des primes d'assurance.

Le cadre d'analyse, correspondant à une implication conduisant à l'action et des actions renforçant l'implication, apparait désormais comme réducteur. La partie suivante va définir la méthodologie d'une étude empirique que nous avons conduite dans plusieurs PME afin d'approfondir ces aspects

II. LA MÉTHODOLOGIE ADOPTÉE

Il a été choisi d'adopter une méthodologie qualitative (Baumard et Ibert, 2003 ; Klein et Myers, 1999 ; Yin, 2008) ainsi qu'une approche interprétative (Walsham, 1995, 2006), pour de nombreuses raisons : Premièrement, nous désirions avant tout étudier les facteurs d'implication et d'action des dirigeants de PME et la répartition des rôles entre les divers acteurs dans le domaine de la SSI. Or, Mucchielli (1996) définit une méthodologie de recherche qualitative comme "*une stratégie de recherche utilisant diverses techniques de recueil et d'analyse qualitatives dans le but d'expliquer, en compréhension, un phénomène humain ou social*" (p.129). Deuxièmement, Coles-Kemp (2009) considère que vu le manque de travaux actuels, les recherches organisationnelles et sociales dans le domaine de la SSI "*requièrent de mener un nombre considérable d'études de cas*" (p. 185). Cette recherche a consisté en l'étude de 8 cas (Eisenhardt, 1996) de PME. Plusieurs entretiens ont été menés dans chaque entreprise : le dirigeant, la personne en charge du S.I. si elle existait, et des salariés. Pour chaque entreprise, deux ou trois salariés dont au moins un cadre si possible étaient désignés par le dirigeant, afin de s'assurer de leur disponibilité et de leur collaboration. Notre "parrainage" par le dirigeant a amené les interviewés à parler plus en confiance.

La liste initiale comportait 920 PME de 20 à 200 salariés, conformément à la typologie établie par Julien et Marchesnay (1996), obtenues à partir du fichier des entreprises de la CCI locale. Deux autres critères ont permis de mieux cibler les entreprises : afin de faire ressortir l'influence du dirigeant, n'ont été conservées que celles dont le siège était local ; ont aussi été éliminées les entreprises du secteur informatique, car une culture "technique" aurait pu biaiser les résultats. Un courrier a été envoyé aux 530 entreprises sélectionnées, leur proposant de participer à cette étude. Huit entreprises sur 510 (20 entreprises n'existaient plus) ont répondu favorablement, soit un taux de réponses positives de 1,6%. Sept entreprises ont décliné l'offre, évoquant toutes un manque de temps, ce qui explique en partie le faible taux de réponses. Une autre explication est donnée par Kotulic et Clark (2004) qui soulignent que peu d'entreprises acceptent de parler de la SSI car elle constitue selon eux un sujet "envahissant" et "importun". Notre objectif étant de mener une étude qualitative, un nombre de cas égal à huit nous a paru suffisant. Dans ces 8 entreprises, 29 entretiens semi-directifs ont été réalisés. Un guide d'entretien a été constitué pour chaque type d'acteur, comportant sept thèmes principaux divisés en sous-thèmes, ce qui correspondait à une vingtaine de questions. Les questions principales et les questions de relance ont été construites afin de vérifier les facteurs de motivation et les freins à l'implication et/ou à l'action des dirigeants. Il était prévu dès le départ de trianguler les discours (Klein et Myers, 1999), dans le but de vérifier le partage réel des rôles et qui était le véritable instigateur des actions mises en place.

Après avoir pris des engagements sur la confidentialité des propos échangés, les entretiens, d'une durée de 30 à 60 minutes suivant les types d'acteurs, ont été enregistrés.

Voici les sept principaux thèmes abordés, entre parenthèses figurent les éléments plus visés par les questions :

- la vision de la sécurité (implication)
- le rôle déclaré par l'acteur (implication, action)
- la vision du rôle des autres acteurs (croisement des discours)
- le comportement des salariés (croisement des discours)
- les facteurs d'implication et d'action et freins (implication, action)
- les actions mises en place ou avis sur les actions mises en place (action et croisement)
- les sinistres observés (implication, action)

Notre objectif était d'évaluer les niveaux d'implication et d'actions du dirigeant, ainsi que d'identifier les facteurs positifs et négatifs pouvant les affecter.

Dans ce but, au travers du guide d'entretien, plusieurs thèmes ont été abordés. Par exemple, dans le thème "vision de la sécurité", nous avons questionné le dirigeant sur son vécu, personnel ou professionnel. Le contexte de l'entreprise a aussi été évoqué, permettant de déterminer si le niveau de concurrence perçu par le dirigeant était important ou non, s'il percevait les enjeux que représentait la SSI pour son entreprise et enfin s'il avait estimé la valeur de ses fichiers (notamment client et comptable) et de ses informations en général. Le niveau de connaissances du dirigeant en S.I. et SSI a été évalué durant tout l'entretien par l'intermédiaire de questions techniques et de questions concernant la compréhension de certaines problématiques organisationnelles et humaines. Le dirigeant a été amené à évoquer ses principales craintes en termes d'incidents de SSI.

Une des questions correspondait à une demande d'évaluation par le dirigeant de son degré d'implication dans la SSI de son entreprise, suivie d'une autre question concernant les éléments concrets qui pouvaient traduire cette implication. En plus de son auto-évaluation, nous avons estimé au travers de l'entretien sa perception de l'importance de la SSI et identifié quels éléments pouvaient l'avoir influencée. Cette évaluation du niveau d'implication était affinée par la perception des autres acteurs à qui nous demandions le rôle que jouait le dirigeant et s'il apportait un soutien, des encouragements ou s'il essayait de "faire passer un message" concernant la SSI dans son entreprise.

Il en est de même pour les actions des dirigeants : après avoir posé des questions générales sur les actions mises en place en termes de SSI, nous avons demandé lesquelles le dirigeant avait mises en place personnellement. Nous avons ensuite vérifié auprès des autres acteurs de l'entreprise que le dirigeant ne s'attribuait pas (ou en partie) les actions menées par un autre, et si elles avaient été perçues à un même degré par les salariés. Par exemple, si le dirigeant nous disait qu'il abordait la SSI lors d'un entretien annuel avec ses salariés, nous demandions ensuite aux salariés s'ils avaient eu ce genre d'échange avec leur dirigeant.

Les "freins à une meilleure SSI" sur un plan général ont tout d'abord été abordés, puis plus spécifiquement les "freins aux actions" en SSI.

L'entretien était poursuivi par la tentative d'obtention de données chiffrées (budgets, journées de formation, publics touchés par les communications sur la sécurité, etc.). Il se terminait par une question au dirigeant portant sur son souvenir de problèmes ayant affecté le fonctionnement de son entreprise, les conséquences, les mesures prises, les sanctions éventuelles envers les responsables, etc.

Des fiches d'entretiens comportant des éléments sur le contexte ont complété les informations enregistrées. Elles ont aussi servi à prendre en compte certaines caractéristiques (âge, ancienneté, niveau d'études…). Un ensemble d'analyses de discours ont été réalisées en accord avec la méthodologie proposée par Miles et Huberman (2003) : trois matrices interentreprises (une par type d'acteur) et huit matrices intra-entreprises ont été créées. Les étapes suivantes d'analyse des données ont été effectuées :

- Retranscription des entretiens, qui s'est traduite par plus de 200 pages de textes ;
- Codage : résumés des entretiens, en utilisant des codes de couleurs par thèmes et détermination des unités de sens (mots, phrases ou expressions relatives à un thème), dans huit matrices intrasite (une par entreprise), incluant des observations personnelles ainsi que certaines phrases remarquables ou particulièrement illustratives ;
- Analyses : combinaison des matrices intrasite au travers du développement de matrices intersites couvrant les constantes et les principales composantes de chaque matrice initiale. Nous avons ensuite établi des méta-matrices. Nous avons croisé les discours des divers acteurs ;
- Interprétation et élaboration des résultats : cette étape concerne les analyses des méta-matrices.

Au total, vingt-quatre tableaux d'analyse ont été établis, soit pour condenser les données (Miles et Huberman, 2003) afin de détailler un thème précis, soit pour croiser certaines informations (Klein et Myers, 1999).

III. LES RÉSULTATS DE L'ÉTUDE

En première partie, nous étudions l'implication et les actions des dirigeants, avec les facteurs positifs et négatifs associés. En deuxième partie, quatre situations correspondant au niveau d'implication et l'action de chaque dirigeant sont mises en évidence. La dernière partie est consacrée à l'identification d'un salarié qui va, suivant certaines conditions, prendre en charge de manière informelle la SSI de son entreprise.

III.1. Détermination des facteurs pouvant influencer l'implication et l'action

Les caractéristiques des entreprises étudiées figurent en Annexe A. Une présentation des huit cas, qui résume les matrices et tableaux d'analyse, est visible en Annexe B.

L'annexe C synthétise les réponses des dirigeants aux questions posées concernant (1) leur vision de la sécurité et les éléments constituant pour eux des motivations ou des freins à leur implication et à leurs actions (2) les actions qu'ils ont conduites dans leurs entreprises et (3) une estimation du niveau d'implication et d'action de chaque dirigeant, avec en gras l'avis du chercheur.

Afin de limiter des biais éventuels relatifs aux déclarations des dirigeants, leurs discours ont été croisés avec ceux des salariés (par exemple pour vérifier l'influence du dirigeant sur eux ou bien qui était la personne à contacter en cas de problème) et des personnes qui s'occupaient de la SSI dans l'entreprise (pour éviter que le dirigeant s'attribue leurs actions).

Il ressort de notre étude que les dirigeants non impliqués n'ont pas pu évoquer d'éléments personnels précis ou d'éléments de contexte (voir le verbatim en Annexes B et C). Par contre, des éléments sont évoqués plus précisément par les dirigeants impliqués : certains facteurs tels que le passé personnel et professionnel du dirigeant, ou l'attachement à son entreprise, apparaissent comme importants pour expliquer l'implication du dirigeant dans la SSI. La perception de la concurrence, la notion de valeur des informations, et les sinistres précédents ("effet vaccin", qui est toutefois limité au fait d'éviter qu'un incident se reproduise) ont aussi été évoqués par les dirigeants en tant que facteurs d'implication dans la SSI de leur entreprise.

La taille de l'entreprise n'est pas reliée à un niveau d'implication ou d'action : les deux plus grandes entreprises de 70 et 130 salariés correspondent respectivement à "implication faible/action moyenne" et "implication moyenne/action faible", alors que dans les plus petites PME on rencontre aussi bien "implication forte/action forte" que "faible implication /faible action".

Un faible niveau en informatique ne semble pas être la cause d'une faible implication ou d'un faible niveau d'action : si les dirigeants des entreprises 2, 6 et 8 (peu impliqués) ont un niveau technique très faible, c'est aussi le cas des dirigeants des entreprises 1, 5 et 7 (impliqués). Pour l'action, la dirigeante de l'entreprise 6 agit (par obligations normatives), tout comme les dirigeants des entreprises 1 et 7 (l'implication prendrait alors le dessus). Par contre, de bonnes connaissances en informatique peuvent être associées à une bonne implication, c'est le lot de tous les dirigeants dans ce cas (entreprises 3, 4 et 7).

Le manque de temps et d'argent, ou encore des priorités "autres" vont limiter les actions des dirigeants impliqués, mais vont jusqu'à bloquer les actions éventuelles des dirigeants peu impliqués.

III.2. Les quatre situations identifiées

Après un retour sur l'ensemble des 29 entretiens et les deux tableaux en An-

Tableau 1 : Positionnement des dirigeants d'entreprises selon les 4 situations identifiées

	Inaction ou action faible	Action
Non impliqué ou peu impliqué	A Entreprise 2 Entreprise 8	B Entreprise 6
Impliqué	C Entreprise 3 Entreprise 5	D Entreprise 1 Entreprise 4 Entreprise 7

nexe C, quatre situations ont pu être identifiées, qui sont représentées dans le tableau 1 ci-dessus[3] :

Afin de vérifier l'impact de ces quatre situations, nous les avons mises en balance avec notre appréciation de l'état de la SSI de chaque entreprise : l'entreprise est-elle en danger ou non ?

La situation "A" correspond au cas d'un dirigeant qui n'est pas impliqué et n'agit pas (entreprises 2 et 8). Cette situation correspond à une SSI très faible dans ces deux PME, car des opérations de base telles que les sauvegardes posent de graves problèmes (non faites, pas d'historique, pas de simulations), les mots de passe sont soit absents soit très courts (de 2 à 5 caractères) et ne sont jamais modifiés, les mises à jours ne sont pas réalisées, on constate une absence majeure de procédures, etc.

Dans tous les autres cas, la SSI dans les entreprises est satisfaisante, la palme revient sans surprise à l'entreprise 3 (cf. Annexe A) : du fait de la taille de cette PME (130 salariés), elle est la seule à pouvoir se reposer sur un professionnel responsable du S.I. (RSI). C'est dans cette entreprise que l'on rencontre le plus de systèmes techniques et automatisés, de procédures organisationnelles précises ainsi qu'une véritable charte de sécurité qui a été signée par tous les salariés. La présence du RSI compense les niveaux d'implication et d'actions, tous deux moyens, de la dirigeante.

Le dirigeant de l'entreprise 1, dépendant de manière vitale de son fichier client, n'a pas hésité à consacrer un budget conséquent pour le protéger. Pour l'entreprise 4, la dirigeante, qui a un bon niveau technique, a su mettre en place des mesures de sécurité satisfaisantes. Dans l'entreprise 5, le dirigeant agit très peu mais il est secondé par un salarié qui a réussi à prendre en charge correctement la sécurité de l'entreprise.

La dirigeante de l'entreprise 6 doit respecter des obligations relatives au domaine de la santé : les contraintes en termes de confidentialité au sujet des patients sont très fortes et la disponibilité informatique tire profit des

[3] Il faut évidemment relativiser la position des dirigeants dans ce tableau. Par exemple, la dirigeante de l'entreprise 3 a un niveau d'action plutôt "moyen moins" (voir Annexe C), ce qui la positionne dans la situation C mais proche de la situation D.

Tableau 2 : Recoupement des niveaux d'implication et d'action, de la personne en charge, et estimation de l'état de la SSI de la PME

Entreprise	1	2	3	4	5	6	7	8
Situation	D	A	C	D	C	B	D	A
Implication[4]	+	-	M	+	M	-	M	-
Action	+	-	-	+	-	M	M	-
Prise en charge	Dirigeant	Conseiller en création	RSI	Dirigeant	Responsable qualité	Dir.+Ext.	Dir.+Ext.	Dessinateur
Etat de la SSI	Satisfaisant	Insuffisant	Satisfaisant	Satisfaisant	Satisfaisant	Satisfaisant	Satisfaisant	Insuffisant

contraintes de disponibilité médicales. Enfin, la dirigeante de l'entreprise 7 est pénalisée par son niveau de connaissances en S.I. Il y a peu de procédures implémentées, mais la SSI de l'entreprise 7 est améliorée par une gestion satisfaisante du prestataire externe, qui a mis en place de bonnes protections "techniques".

Le tableau 2 résume les situations rencontrées et fait apparaître la personne qui prend en charge la SSI de l'entreprise.

Il est enfin à noter qu'aucune entreprise n'utilisait de norme ou de méthode spécifique à la sécurité des S.I.

III.3. La prise en charge informelle de la SSI par un salarié

Dans le tableau 2, on remarque que parfois, un salarié prend en charge la SSI de l'entreprise (entreprises 2, 5 et 8). Cette prise en charge informelle du SI et surtout de sa sécurité n'avait pas été prévue. Le salarié, que nous avons baptisé ensuite le "salarié-RSSI" (responsable de la SSI) était présenté par le dirigeant comme "*le salarié qui s'en occupe*" ou "*celui qui s'y connait*". L'étude étant qualitative, il a été possible d'adapter les guides d'entretiens : cette personne était à la fois un "salarié" et un "responsable informatique". Les questions des deux guides ont donc été utilisées, et il a été possible d'identifier les interactions de ces "hybrides", non seulement avec le dirigeant mais aussi avec les autres salariés de l'entreprise, ainsi que les rôles joués par ces salariés.

Les fonctions réelles de ces salariés-RSSI sont respectivement "conseiller en création d'entreprise", "responsable qualité" et "dessinateur industriel". L'annexe D présente les éléments les plus significatifs que l'on peut tirer de leurs entretiens.

Ces trois salariés n'avaient pas ou peu de compétences initiales et se sont auto-formés pour remplir leur rôle. Leurs motivations correspondent avant tout à la compréhension des pertes pos-

[4] - = Faible, M = Moyen, + = Fort.

sibles : "*on sait ce que cela représente*", "*je connais le problème*". Et ils considèrent qu'il est de leur devoir d'aider leur organisation : ce sont eux qui gèrent les relations avec les prestataires extérieurs, mais ce n'est pas toujours simple car ils manquent de compétences : "*j'ai un niveau vraiment moyen*", "*je peux le faire si c'est pas trop compliqué*", "*j'ai appris l'informatique pour pouvoir me passer des informaticiens*".

Dans les entreprises où les dirigeants ne sont pas impliqués (entreprises 2 et 8), ils doivent gérer des relations parfois difficiles avec leur dirigeant : "*Elle a des comportements dangereux dont elle ne se rend même pas compte*" ou bien "*il s'investit pas, je n'ai pas le budget que je veux pour faire ce que je veux*" ou encore "*je dois batailler*". Les dirigeants vont même jusqu'à refuser d'utiliser des mots de passe ou à faire annuler leur changement régulier, ou bien encore refuser l'achat d'un serveur pour mettre en place une sauvegarde centralisée, contre l'avis du salarié-RSSI. Dans ces deux entreprises, il y a aussi un problème dans les relations avec les autres salariés. Ils leur demandent d'exécuter certaines actions, comme faire de temps en temps des sauvegardes et/ou de lancer un antivirus, mais ils ont du mal à se faire entendre : "*il n'y a pas grand monde qui l'a fait*" ou "*j'ai essayé de faire ce qu'il faut pour que les gens fassent leurs sauvegardes mais j'ai pas envie de me mettre à les faire à leur place, surtout qu'à la limite l'informatique c'est pas mon boulot d'origine*". On en arrive à des comportements fatalistes : "*J'essaie de responsabiliser chacun, et puis après, s'il se passe quelque chose, on verra bien ce qu'il se passe*".

Dans l'entreprise 5, la situation est meilleure : le dirigeant n'agit pas plus mais son implication fait qu'il désire être au courant de tout. "*Je rapporte ce qu'il y a à M. [le dirigeant], et il me dit bon, il faut contacter notre société informatique*". Le salarié-RSSI arrive donc à avancer avec son dirigeant, et son dirigeant a confiance en lui. Durant l'entretien, le salarié-RSSI se référait souvent à lui "*ça c'est [le dirigeant] qui pourra vous répondre*". Il ne rencontrait pas non plus de problèmes avec les salariés, qui respectaient ce que demandait le salarié-RSSI (prudence quant à la confidentialité, faire ses sauvegardes, etc.).

IV. DISCUSSION DES RÉSULTATS

Dans un premier temps, nous faisons le point sur les facteurs relatifs à l'implication et à l'action que nous avons identifiés et nous les confrontons au seul modèle que nous avons pu identifier dans la littérature dans le domaine de la SSI. Dans un second temps, une étude est réalisée sur le rôle du salarié qui a pris en charge de manière informelle la SSI de son entreprise. Les quatre situations du tableau 1 (§3.2) sont ensuite analysées, avec une étude du partage des rôles des divers acteurs, ce qui nous amène ensuite à proposer des recommandations pour améliorer la SSI dans les PME.

IV.1. Les facteurs relatifs à l'implication et à l'action

Les résultats présentés dans le §3.1 remettent partiellement en question le modèle de Goodhue et Straub (1991) examiné en figure 1 (§1.1), dont voici les principales lacunes :

1. L'influence majeure du passé personnel et professionnel et de l'attachement à l'entreprise sur l'implication du dirigeant ;
2. La faible influence des actions "directes" sur l'implication du dirigeant. Nos entretiens font plutôt ressortir une implication qui influence les actions "directes" et "indirectes". Le lien de causalité existant en figure 1 doit donc être inversé ;
3. Si le dirigeant peut se reposer sur une tierce personne, il agira moins de manière directe, même s'il est impliqué. Par contre son implication n'en sera pas affectée. Ceci renforce le point précédent ;
4. La perception de la priorité d'autres actions va aussi limiter voire bloquer les actions directes des dirigeants.

Au sujet du deuxième point ci-dessus, l'influence des mesures prises (actions précédentes) sur l'implication du modèle de Goodhue et Straub (1991) ne reflète pas bien le cas du dirigeant non impliqué : il n'agira pas et ne peut sortir du cercle vicieux dans lequel il n'est pas impliqué. Par contre un dirigeant peu impliqué et obligé d'agir va-t-il finir par vraiment s'impliquer ? La dirigeante de l'entreprise 6 n'était toujours pas impliquée après 5 ans d'ancienneté et d'action forcée : cette "action forcée" n'est pas apparue comme une source d'implication.

Les autres éléments du modèle de Goodhue et Straub ont pu être vérifiés, c'est-à-dire premièrement l'influence positive sur l'implication des dirigeants de leurs croyances au sujet des pertes qu'ils pourraient subir, ainsi que l'influence positive de leur perception d'une forte concurrence sur cette implication ; deuxièmement, le niveau de connaissances en S.I. va correspondre à une plus grande implication du dirigeant dans la SSI de son entreprise, mais va aussi jouer un rôle dans les actions qu'ils vont mettre en place.

Deux autres points sont à noter :

1. L'obligation de respecter des normes ou méthodes aura un effet fort sur les actions directes du dirigeant, mais deux éléments vont relativiser son intérêt : premièrement peu de PME sont soumises à ces obligations et deuxièmement la norme ou méthode ne sera pas forcément spécifique à la SSI et ne couvrira donc pas systématiquement toutes les actions à mettre en place ;
2. Même si la littérature montre que les femmes, les personnes de moins de 45 ans et les plus diplômés sont plus concernés par la SSI que les autres personnes, les données signalétiques (sexe, âge, diplôme) de l'annexe C n'ont pas d'influence notable, dans les cas étudiés, sur une quelconque implication ou action. Par exemple, la dirigeante de l'entreprise 2, pourtant de niveau Bac+5, n'est pas du tout impliquée et n'agit pas. Même si ces éléments pourraient constituer des variables modératrices, ils paraissent secondaires face aux autres éléments identifiés.

Ces divers facteurs permettent de mieux comprendre pourquoi le dirigeant va être impliqué et/ou agir dans la SSI de son entreprise. Toutefois, avant d'analyser les quatre situations d'implication et d'actions identifiées dans la partie consacrée aux résultats, il s'avère utile de mieux comprendre le rôle du salarié-RSSI qui va seconder, voire parfois même se substituer au dirigeant dans la prise en charge de la SSI.

IV.2. Le rôle du salarié-RSSI

Quand le dirigeant n'était pas impliqué (situations de type "A"), même si le dirigeant n'agissait pas ou très peu, à chaque fois un salarié prenait malgré tout en charge le S.I. de l'entreprise et sa sécurité. L'article de Stemberger *et al.* (2011) permet de mieux appréhender les problèmes évoqués par les salariés-RSSI dans les entreprises 2 et 8 : le manque d'implication du dirigeant explique le fait qu'il ne soutient pas son salarié-RSSI, ce qui entraîne que la position hiérarchique de ce dernier n'est pas affirmée. Si l'on ajoute à ceci que la fonction du salarié-RSSI n'est qu'informelle (il n'est aux yeux de tous qu'un salarié comme les autres) et que de plus il n'a pas de diplôme pour légitimer ses compétences, il ne dispose ni de l'autorité ni de la crédibilité nécessaires pour assurer sa fonction (Stemberger *et al.*, 2011). Sous cet éclairage, on comprend mieux que dans les entreprises 2 et 8 les salariés-RSSI n'arrivent pas à compenser le manque d'action du dirigeant (voir Annexe D), car l'efficacité de leurs actions est en grande partie annihilée par leur absence de pouvoir réel. Par contre, il n'est pas exclu que dans des situations de type "A" certains salariés, dotés par exemple d'un grand pouvoir de conviction ou d'un grand charisme, puissent malgré tout s'imposer et arriver à mettre en place une SSI satisfaisante.

Dans une situation de type "C" où le dirigeant est impliqué, le salarié-RSSI de l'entreprise 5 n'évoque aucun problème lié à la mise en œuvre de ses suggestions, que ce soit vis-à-vis des autres salariés ou vis-à-vis du dirigeant. Il y avait une bonne collaboration entre le dirigeant et le salarié-RSSI, ainsi qu'une bonne convergence de leurs discours. Tout au plus l'entretien du salarié-RSSI laissait transparaître le "poids" de son dirigeant dans les décisions : ce poids était lié à la fois aux préoccupations du dirigeant en termes de SSI et à son grand charisme. Dans cette entreprise, le salarié-RSSI compensait donc de manière efficace le manque d'actions directes de son dirigeant, et la SSI de l'entreprise était satisfaisante.

Afin de compléter cette notion de soutien du dirigeant, un des principaux résultats de l'étude de Stemberger *et al.* (2011) correspond au fait que le personnel en S.I. peut obtenir le soutien de son dirigeant si "*son rôle, ses connaissances et compétences sont adéquates*" (p. 434). Les connaissances correspondent ici aux savoirs en termes de management et de métier. Afin d'améliorer la situation des salariés-RSSI, il s'agirait donc surtout de clarifier et/ou de mieux formaliser leur rôle, ainsi que de développer les compétences techniques perçues par les dirigeants de ces salariés, qui sont souvent autodidactes en S.I et SSI.

Un point positif est que même si les connaissances techniques sont encore une priorité des dirigeants lors du recrutement d'un RSI, Litecky *et al.* (2004) ont montré que les "soft-skills", c'est-à-dire, la gentillesse, l'aptitude à communiquer, les capacités au travail en équipe et à s'intégrer à l'organisation, sont jugées comme les plus importantes quand on évalue un RSI. Donc même si les compétences des salariés-RSSI ne sont pas toujours bien perçues, ils pourraient tout de même être bien jugés grâce à leurs autres qualités personnelles ?

Cette compréhension du rôle et du poids du salarié-RSSI permet de passer à une étude plus globale du partage des rôles dans la gestion de la SSI.

IV.3. Analyse des quatre situations identifiées

Dans un premier temps, nous analyserons les relations entre les acteurs impliqués dans la SSI d'une PME, puis nous examinerons quelques pistes d'amélioration de la SSI dans les PME.

IV.3.1. Les quatre situations et les rôles des acteurs impliqués

Les acteurs qui entrent en jeu dans le cadre de la SSI des PME sont :

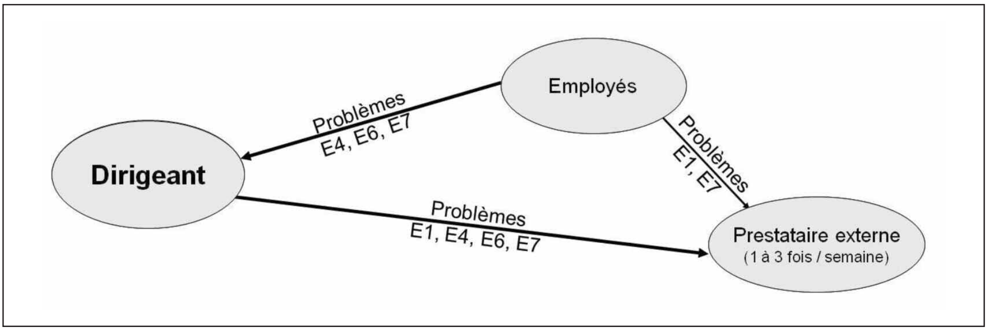
- le dirigeant ;
- un RSI, pour les plus grosses PME (un seul cas ici) ;
- un prestataire extérieur, pour les PME sans RSI ;
- dans certaines PME, un salarié-RSSI, qui a décidé de prendre en charge le SI et la SSI de son entreprise.

Il s'agit maintenant d'entrer dans le détail des relations entre ces acteurs. Dans les situations "B" et "D", le dirigeant agit directement (figure 2) : il va traiter tout ce qui touche à la SSI par lui-même, en faisant appel à son prestataire externe. Dans les entreprises 4 et 7, le dirigeant a suffisamment de compétences pour diagnostiquer et résoudre certains problèmes, même si dans l'entreprise 7, les employés vont parfois court-circuiter le dirigeant dans les situations les plus basiques. Dans le cas de l'entreprise 1, les employés appellent directement le prestataire externe, car le dirigeant est peu compétent techniquement. Mais ce dirigeant contacte lui-même le prestataire pour les investissements importants (ex : c'est lui qui est à l'origine de la mise en place d'un système de disques redondants). Dans les entreprises 1, 4 et 7, les actions indirectes des dirigeants, telles que les rappels en SSI auprès des salariés, sont bien présentes.

Le cas de l'entreprise 6 est plus particulier : la dirigeante n'étant pas impliquée, elle se contente de mettre en place les actions obligatoires (cadre des établissements de santé). Elle gère les problèmes non urgents des salariés, même si en cas de blocage et d'urgence ces derniers peuvent exceptionnellement appeler directement le prestataire externe pour gagner du temps (Figure 2).

Dans les situations "A" et "C", le dirigeant n'agit pas directement (figure 3), les salariés font remonter les problèmes au salarié-RSSI. Le dirigeant de l'entreprise 5 étant impliqué, il souhaite valider toute décision de son salarié et va en grande majorité soutenir ces décisions ainsi que renforcer sa position auprès des autres salariés (actions indirectes).

Figure 2 : Relations inter-acteurs quand le dirigeant agit directement



Dans la situation "A", qui est celle des entreprises 2 et 8, le dirigeant laisse agir le salarié-RSSI sans réel contrôle. Quand le salarié-RSSI désire mettre en place quelque chose allant au-delà de la résolution des simples problèmes, le salarié non seulement doit "batailler" avec le dirigeant, mais a de plus peu de chances de se voir écouté par le dirigeant ou ses collègues (figure 3).

Toujours dans la situation "C" où le dirigeant n'agit pas directement, on rencontre aussi le cas du RSI officiel de l'entreprise 3, qui est plus classique (figure 4).

La dirigeante de l'entreprise 3 est moyennement impliquée dans la SSI de son entreprise (Annexe C). Ses actions indirectes concernant des rappels sur la SSI sont limitées à ses collaborateurs proches, même chose pour la notation

Figure 3 : Relations inter-acteurs quand le dirigeant n'agit pas directement (salarié-RSSI)

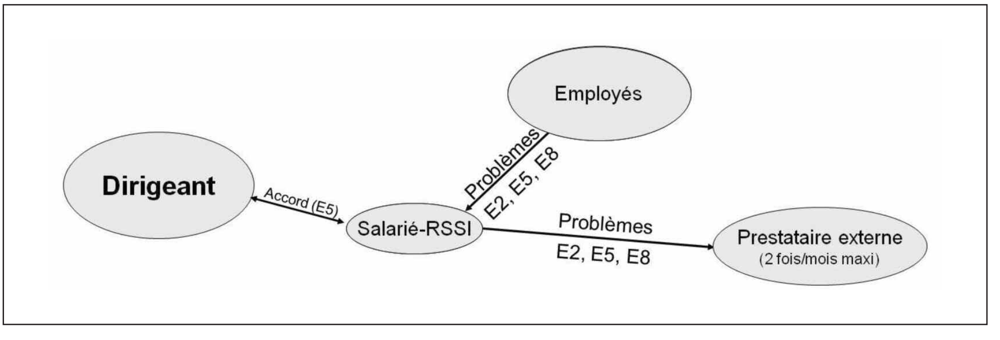
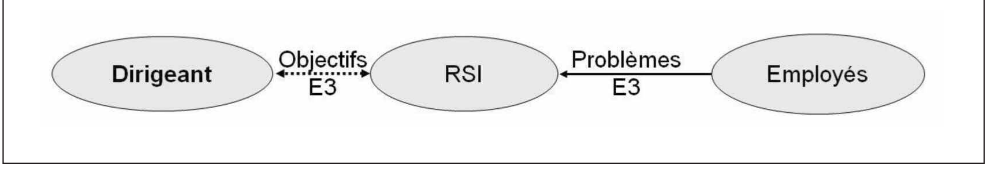


Figure 4 : Relations inter-acteurs quand le dirigeant n'agit pas directement (RSI officiel)



des salariés. Il n'y a donc pas de "rayonnement" dans toute l'entreprise qui permettrait une plus grande sensibilisation des salariés, même si le RSI a fait signer à tous une charte de sécurité. Autre type d'actions indirectes : la dirigeante, même si elle se décharge entièrement sur son RSI, lui a assigné des objectifs précis et suit ses résultats régulièrement. Le manque d'actions directes de la dirigeante est largement compensé par le RSI qui est très dynamique et proactif.

Il est difficile de trancher sur l'inactivité du dirigeant : il nous a plutôt semblé que le salarié-RSSI est apparu parce que le dirigeant n'agissait pas, et dans le cas d'un vrai RSI, le dirigeant n'agissait pas parce qu'il faisait toute confiance à son RSI.

L'implication apparaît comme étant déterminante pour qu'une entreprise puisse atteindre un niveau de SSI satisfaisant. En effet, en addition aux actions indirectes, cette implication va aussi faciliter les actions directes des dirigeants. En cas de manque d'actions directes de leur part, des mécanismes de compensation vont apparaître dans l'organisation, qui seront d'autant plus efficaces si le dirigeant est impliqué.

IV.3.2. Comment améliorer la SSI dans chacune des quatre situations ?

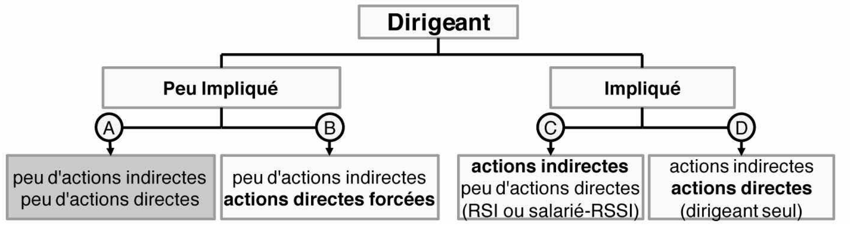
Les quatre situations vont maintenant être réexaminées dans l'optique d'une amélioration de la SSI dans les PME.

Dans la situation "D", le dirigeant va agir à la fois de manière indirecte et directe, les seules limites seront liées à l'échelle de ses priorités. Son niveau technique ne sera pas véritablement un handicap car il pourra acquérir des connaissances supplémentaires grâce à ses interactions avec son prestataire extérieur. Comme le dirigeant est impliqué, il sera possible d'agir sur sa perception des priorités par une sensibilisation complémentaire aux pertes possibles par exemple. Son niveau de connaissances pourra aussi être développé par une formation, dans l'optique d'améliorer sa réflexion stratégique pour arriver à mieux lier stratégie d'entreprise et SSI.

Dans la situation "C", un niveau faible d'actions directes du dirigeant sera compensé par une tierce personne (RSI ou salarié-RSSI). Ce sera surtout la sensibilisation du dirigeant aux actions indirectes qui va compter. Dans le cas d'une PME dans laquelle il y aura un responsable du SI, ce RSI n'aura pas de problème pour mettre en place des mesures de SSI, d'autant qu'il aura toute la légitimité pour se faire entendre du dirigeant. Dans le cas d'un salarié-RSSI, il faudra en plus s'assurer d'une bonne collaboration entre les deux acteurs, et améliorer la tâche du salarié-RSSI. Une formation complémentaire ou une validation des acquis assiéra mieux ses compétences techniques, tandis qu'un aménagement plus formel de son travail (part de sa charge en SSI comparée à son métier "officiel") et/ou une valorisation de sa tâche faciliteront sa reconnaissance dans l'entreprise.

Dans la situation "B", le dirigeant va manquer d'actions indirectes car il ne sera pas impliqué, mais il effectuera certaines actions directes "forcées". La qualité de la SSI de son entreprise sera fortement liée aux éléments obligatoires de la norme qu'il aura dû implémenter.

Figure 5 : Les actions directes et indirectes selon la situation



Dans cette situation, comme pour la situation "A" examinée ci-après, il apparaît difficile de sensibiliser un dirigeant non impliqué puisqu'il n'est pas en recherche d'informations ou de sensibilisations relatives à la SSI. Il ne reste qu'à espérer qu'à force d'agir il finira par s'impliquer peu à peu, même si nous n'avons pas constaté un tel effet. Une autre possibilité, mais difficilement réalisable, serait de compléter certaines normes, comme dans le cas de l'entreprise 6 où la confidentialité des informations concernant les patients hospitaliers devait être assurée, par des éléments garantissant une sécurité au moins basique (l'entreprise 6 avait des lacunes en termes de procédures de sauvegarde et d'archivage des informations). La dernière possibilité serait un "effet vaccin", c'est-à-dire un incident suffisamment important pour ouvrir les yeux du dirigeant, sans pour cela impliquer des conséquences trop graves pour la PME.

Pour les situations "A" et "B", comme le dirigeant n'agit pas suffisamment, que ce soit de manière indirecte ou directe, il s'agirait alors soit de favoriser l'apparition d'un salarié-RSSI, en faisant comprendre au dirigeant qu'une personne pourrait assurer, en plus de ses tâches, au moins le strict minimum en termes de SSI, et ce "gratuitement", soit de mieux valoriser un salarié-RSSI s'il existe déjà, comme cela a été évoqué précédemment.

Dans la situation "A", si personne n'agit ou si le salarié-RSSI n'a pas les moyens de compenser le manque d'actions du dirigeant, on risque d'en arriver au cas qui était évoqué par la dirigeante de l'entreprise 4 : le cas d'une entreprise dans laquelle il n'y avait pas de firewall, pas d'antivirus, pas de sauvegardes ni de mots de passe, aucune procédure, avec de très gros risques de pertes d'informations, bref, une entreprise en sursis… Dans les 8 entreprises (voir tableau 2), il y avait toujours quelqu'un qui gérait la SSI : nous avons rencontré un RSI (dans la plus grande des PME), trois salariés-RSSI, et enfin quatre dirigeants qui géraient la SSI par eux-mêmes (dont un de manière "forcée").

La figure 5 reprend les quatre situations ainsi que les actions, indirectes ou directes qui correspondent :

Dans les plus petites PME, le dirigeant aura plus de chances d'avoir à gérer seul la SSI de son entreprise. Un dirigeant impliqué agira donc principalement de manière directe (par exemple gestion du prestataire extérieur, mise en place de mesures de SSI), et renforcera son action par quelques actions indirectes qui vont influencer les salariés (valorisation des bons comportements ou insistance sur les comportements à adopter).

Dans des PME de plus grande taille on trouvera des responsables du SI voire de la SSI, qui prendront en charge les actions directes. Dans ce cas, un dirigeant impliqué va agir de manière indirecte afin de gérer ce responsable officiel en travaillant de concert avec lui et/ou en contrôlant son activité. Dans d'autres PME où il n'existe pas de responsable officiel, un salarié-RSSI aura pu émerger. Dans ce cas un dirigeant impliqué pourra agir comme dans le cas d'un véritable RSI, mais en plus il lui donnera, grâce à son soutien, la crédibilité et l'autorité qui pourraient être limitées du fait de son rôle informel. Tout comme dans le cas du "dirigeant seul", on observe les autres actions indirectes d'influence ou de renforcement des comportements relatifs à la SSI des salariés.

Si le dirigeant n'est pas impliqué, le dirigeant aura peu d'actions indirectes. Il n'exercera que les actions directes "obligatoires" s'il y est forcé par des lois ou des normes obligatoires. Un seul cas, que nous n'avons pas rencontré, pourrait être synonyme d'une SSI satisfaisante pour une situation de type "A" ou "B" : ce serait le cas d'un RSI "officiel", qui arriverait à mettre en place les mesures nécessaires, en ayant à convaincre à chaque fois son dirigeant de débloquer les budgets correspondants. Dans le cas d'un salarié-RSSI, le manque de soutien du dirigeant aura beaucoup plus de chances d'être préjudiciable car le salarié-RSSI aura non seulement un poste informel, mais de plus souffrira de problèmes de crédibilité et d'autorité vis-à-vis des autres acteurs.

Les diverses possibilités d'amélioration de la SSI dans les PME peuvent être synthétisées ainsi :

- développer le "pouvoir" et le niveau en S.I. d'un éventuel salarié-RSSI ;
- rendre obligatoire l'utilisation d'une méthode, d'une norme ou au moins d'un guide de bonnes pratiques en SSI ;
- faciliter la collaboration dirigeant – société extérieure ;
- renforcer le niveau en SI et SSI du dirigeant et améliorer sa sensibilisation à la SSI.

V. CONTRIBUTIONS

V.1. Contributions théoriques et méthodologiques

Le principal résultat correspond à l'identification de ce salarié-RSSI qui décide d'assumer de manière informelle la responsabilité du SI de son entreprise et de sa sécurité. La nécessité d'un soutien de ce salarié de la part du dirigeant a aussi été mise en évidence.

Une autre contribution de ce travail est l'exploration des relations entre l'implication du dirigeant en SSI et ses actions, peu étudiées dans la littérature en systèmes d'information. En SSI, les études théoriques sont encore plus rares et anciennes puisqu'à notre connaissance seuls Goodhue et Straub (1991) se sont intéressés à ce problème, il y a plus de vingt ans.

Nous avons aussi montré que la simple inférence d'une implication qui entraine l'action doit être dépassée car en réalité les relations entre l'implication et l'action sont complexes : ce sont plutôt des interactions. L'étude qualitative a mis en évidence de nouveaux facteurs relatifs à l'implication et/ou à l'action des dirigeants qui remettent partiellement en question le modèle de Goodhue et Straub (1991). Les éléments identifiés pourront constituer le point de départ d'études quantitatives par exemple.

La troisième contribution de notre travail concerne l'impact de l'implication et de l'action du dirigeant sur la SSI de l'entreprise. Alors que l'idée commune est que l'implication et l'action du dirigeant, les deux étant souvent confondues (Basu *et al.*, 2002) sont des pré-requis pour que la SSI d'une entreprise soit satisfaisante, il s'avère que c'est plutôt l'implication qui sera déterminante. Les actions indirectes, notamment la manière dont le dirigeant va interagir avec son RSI ou un salarié-RSSI, ainsi que l'influence qu'aura un dirigeant impliqué sur ses salariés, sont les plus critiques. Un manque d'implication pourra tout de même être partiellement compensé dans certains cas.

V.2. Contributions pratiques

Sur un plan managérial, notre travail peut servir à mettre en place des campagnes de sensibilisation ou de formations adaptées aux dirigeants. Il s'agirait de leur donner un enseignement de base en S.I., de les sensibiliser aux problématiques relatives à la SSI en les aidant par exemple à estimer la valeur de leurs informations, et de mieux leur faire appréhender les principaux risques auxquels ils auront à faire face ainsi que les conséquences de certains sinistres liés à leur activité et à leur secteur. Les facteurs d'implication et d'action des dirigeants qui ont été identifiés dans cette étude donneront plus d'impact à ces sensibilisations et formations. Mais ceci ne résoudrait pas le problème du dirigeant peu impliqué, qui ne verrait pas l'intérêt de telles sensibilisations.

Cette étude permet de mieux comprendre comment se partagent les rôles en PME. Elle a aussi identifié cette prise en charge de manière informelle de la SSI par des salariés, ainsi que leurs motivations et les problèmes qu'ils rencontrent. Par contre, l'incidence de ce salarié-RSSI a pu s'avérer bénéfique (entreprise 5) ou ne servir à presque rien (entreprises 2 et 8). Ceci met en évidence la nécessité d'informer les dirigeants qu'ils doivent absolument soutenir leur salarié-RSSI quand il existe ; les dirigeants de PME devront non seulement leur accorder un budget, mais aussi une crédibilité auprès des autres salariés, et si possible du temps et/ou une certaine forme de reconnaissance, qu'elle soit financière ou non. Pour ceux n'ayant pas de salarié-RSSI, il serait intéressant de les informer de cette alternative au recrutement d'un professionnel, qui n'est pas souvent à la portée du budget d'une PME (Lee et Larsen, 2009).

CONCLUSION

Cette étude avait pour objectif d'apporter un éclairage sur l'implication et l'action des dirigeants de PME et son importance dans le cadre de l'amélioration de la SSI, qui constitue un domaine sensible et d'actualité dans la littérature en sciences de gestion.

Elle comprend les limites usuelles liées à la méthodologie qualitative adoptée pour étudier ce sujet. Il pose un problème de généralisation des résultats, du fait de conclusions basées sur 8 cas et 29 entretiens, une étude de type quantitatif pourra vérifier et affiner ces résultats si nécessaire. Une autre limite correspond à une possibilité de biais liée à la désignation par le dirigeant des personnes à interroger. D'autres cas d'études de situations de type "B" seraient nécessaires pour mieux comprendre la problématique de l'action forcée. L'explication de l'inactivité d'un dirigeant quand il peut se reposer sur un RSI ou un salarié-RSSI mériterait aussi d'être approfondie.

Enfin, si l'influence de la taille ne semble pas déterminante, l'activité de l'entreprise semble une piste prometteuse. Les entreprises du secteur informatique pourraient être étudiées pour vérifier quelles différences peuvent apparaître au sujet du comportement des dirigeants. Il s'agirait aussi par exemple d'identifier les organisations les plus sensibles à la confidentialité des données ainsi que celles dépendant fortement de la disponibilité et de l'intégrité de leurs informations (plateaux de télévente par exemple), ou bien des entreprises appartenant à des secteurs innovants ou de pointe.

Sur un plan théorique, il serait avantageux de pousser plus loin l'étude des facteurs d'implication et d'action des dirigeants par le biais d'une étude quantitative, et d'identifier plus précisément lesquels vont plus agir sur l'implication, sur les actions directes du dirigeant ou sur les deux à la fois.

Lors de prochaines études, il serait souhaitable de mieux prendre en compte les aspects "SSI obligatoire" que peuvent présenter certaines normes ou législations ainsi que le secteur d'activité de l'entreprise. Il serait aussi intéressant d'identifier les lacunes que peuvent présenter certaines réglementations, pour montrer qu'elles ne sont pas forcément suffisantes et que d'autres mesures de sécurité doivent les compléter. L'utilisation des normes de SSI, parmi les PME de moins de 200 salariés, s'avère malheureusement rare car elles sont en général trop lourdes pour de petites structures (Barlette et Fomin, 2009). A défaut de normes, afin de les aider à adopter de bonnes pratiques, les dirigeants de PME pourraient être informés de l'existence de guides, comme celui de l'ENISA (2009).

La voie juridique est prometteuse, car des lois pourraient obliger les dirigeants, même non impliqués, à mettre en place les actions les plus indispensables. A titre d'exemple, la commission Européenne a fait adopter début 2012 une proposition de réforme visant à harmoniser et durcir les lois actuelles relatives à la protection de la vie privée et du secret professionnel, obligeant à terme les entreprises à mettre en place des procédures spécifiques, et accroissant le montant des amendes jusqu'à 1 million d'euros contre 300.000 € actuellement (Art. 226-17 à 226-22 du code pénal).

Le phénomène de prise en charge de la SSI par un salarié, qui a été mis en évidence lors de l'étude qualitative, mérite qu'une étude spécifique lui soit consacrée. L'étude pourrait prendre en compte les aspects suivants : dans quelles conditions apparaissent les salariés-RSSI ? (et comment faciliter leur apparition), comment pérenniser cette prise en charge informelle ? (prise en compte du travail additionnel, compensations, …). Les rapports de force dirigeant – salarié-RSSI gagneraient aussi à être étudiés. Enfin, quelles qualités sont nécessaires pour un salarié-RSSI, à la fois techniques mais aussi managériales et personnelles ? Des travaux pourraient être consacrés à l'étude d'un "profil idéal" de la personne chargée de la SSI, que ce soit un salarié-RSSI ou bien plus classiquement le RSI de l'entreprise.

RÉFÉRENCES

Anderson, E.E. et Choobineh, J. (2008), Enterprise information security strategies, *Computers & Security*, n°27, p. 22-29.

Ashenden, D. (2008), "Information security management: A human challenge?", *Information security technical report*, n°13, p. 195-201.

Avolio, F.M. (2000), "Best practices in network security: as the networking landscape changes, so must the policies that govern its use. Don't be afraid of imperfection when it comes to developing those for your group", *Network Computing*, Vol. 60, n°20, p. 60-72.

Barki, H. et Hartwick, J. (1989), "Rethinking the Concept of User Involvement", *MIS Quarterly*, Vol. 13, n°1, p. 53-63.

Barlette, Y. (2008), "Une étude des comportements liés à la sécurité des systèmes d'information en PME", *Systèmes d'Information et Management*, Vol. 13, n°4, p. 7-30.

Barlette, Y. et Fomin, V.V. (2009), The adoption of Information Security management Standards: A Literature Review. In Knapp K.J. (Ed.), *Cyber-Security & Global Information Assurance*: Threat, analysis and response solutions, p. 119-140. IGI Global, USA.

Basu, V., Hartono, E., Lederer, A.L. et Sethi, V. (2002), "The impact of organizational commitment, senior management involvement, and team involvement on strategic information system planning", *Information & Management*, Vol. 39, p. 513-524.

Baumard, P. et Ibert, J. (2003), Quelles approches avec quelles données ? In Thiétart R.-A. et coll., *Méthodes de recherche en management*, p. 82-103, Dunod, Paris.

Boss, S.R., Kirsh, L.J., Angermeier, I., Shingler, R.A. et Boss, R.W. (2009), "If someone is watching, I'll do what I'm asked: mandatoriness, control and information security", *European Journal of Information Systems*, n°18, p. 151-164.

Bruce, G. et Dempsey, R. (1997), *Security in Distributed Computing - Did You Lock the Door?*, Hewlett Packard Company, Palo Alto, USA.

CLUSIF, (2004), *Retour sur investissement en SSI : quelques clés pour argumenter.*

Coles-Kemp, L. (2009), "Information Security Management: An entangled research challenge", *Information security technical report*, Vol. 14, n°4, p. 181-185.

Davenport, T. (2002), Privilégier l'information sur la technologie, (accédé le 27 avril 2012) http://www.lesechos.fr/formations/manag_info/articles/article_1_1.htm.

Dhillon, G. et Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, Vol. 11, p. 127-153.

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

Dong, L. (2008), "Exploring the impact of top management support of enterprise systems implementations outcomes", *Business Process Management Journal*, Vol. 14, n°2, p. 204-218.

Dong, L., Neufeld, D. et Higgins, C. (2009), "Top management support of enterprise systems implementations", *Journal of Information technology*, n°24, p. 55-80.

Drugescu, C. et Etges, R. (2008), "Maximizing the return on investment of information security programs: program governance and metrics", *Information systems security*, December, p. 30-40.

Dutta, A. et McCrohan, K. (2002), "Management's role in information security in cyber economy", *California Management Review*, Vol. 45, n°1, p. 67-87.

Eisenhardt, K.M. (1989), "Building theories from case study research", *Academy of Management Review*, Vol. 14, n°532, p. 57-74.

ENISA, (2009), Les dix bonnes pratiques de l'ENISA en matière de sensibilisation à la sécurité, (accédé le 15 février 2012) http://www.enisa.europa.eu/act/ar/deliverables/2009/ar-security-practices-fr/?searchterm=good%20practices.

Forcht, K.A. et Ayers, W.C. (2000), "Developing a computer security policy for organizational use and implementation", *Journal of computer information systems*, Vol. 41, n°2, p. 52-57.

Forte, D. (2008), "Selling security to top management", *Network Security,* March, p. 18-20.

Friend, M. et Pagliari, L.R. (2000), Establishing a safety culture: getting started. *Professional Safety,* Vol. 45, n°5, p. 30-32.

Goodhue, D.L. et 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.

Grover, V. (1993), "Empirically derived model for the adoption of customer-based inter-organizational systems", *Decision Sciences*, Vol. 24, n°3, p. 603-639.

Gupta, A. et 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.

Hagen, J.M., Albrechtsen, E. et Hovden, J. (2008), "Implementation and effectiveness of organizational information security measures", *Information Management and Computer Security*, Vol. 16, n°4, p. 377-397.

Helmich, D.L. et Brown, W.B. (1972), "Successor type and organizational change in the corporate enterprise", *Administrative science quarterly*, Vol. 17, p. 371-381.

Hoff, T. (2008), "The Effect of Senior Management Participative Involvement on Employee Perceptions", *Organization Development Journal*, Vol. 26, n°3, p. 73-87.

Hofstede, G., Neuijen, B., Daval-Ohayv, D. et Sanders, G. (1990), "Measuring organizational cultures: a qualitative and quantitative study across twenty cases", *Administrative science quarterly*, Vol. 35, p. 286-316, Cornell University.

INSEE (2011), *Tableaux de l'Économie Française*, INSEE Références, Paris.

Jarvenpaa, S.L. et Ives, B. (1991), "Executive commitment and participation in the management of information technology", *MIS Quarterly*, Vol. 15, n°2, p. 205-227.

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

Julien, P.A. et Marchesnay, M. (1996), *L'entrepreneuriat*, Economica, Paris.

Kankanhalli, A., Hock-Hai, T., Bernard, C.Y.T. et Kwok-Kee, W. (2003), "An integrative study of information systems security effectiveness", *International journal of information management*, Vol. 23, p. 139-154.

Kayworth, T. et Whitten, D. (2010), “Effective information security requires a balance of social and technology factors”, *MIS Quarterly executive*, Vol. 9, n°3, p. 163-175.

Khoo, B., Harris, P. et Hartman, S. (2010), “Information Security Governance Of Enterprise Information Systems: An Approach To Legislative Compliant”, *International Journal of Management and Information Systems*, Vol. 14, n°3, p. 49-55.

Klein, H.K. et Myers, M.D. (1999), “A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems”, *MIS Quarterly*, Vol. 23, n°1, p. 67-94.

Knapp, K.J., Marshall, T.E., Kelly Rainer, R. et Nelson Ford, F. (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. et Byrd, T.A. (2009), “Information security policy: An organizational-level process model”, *Computers & Security*, n°28, p. 493-508.

Kotulic, A. et Clark, J.G. (2004), “Why there aren’t more information security research studies”, I*nformation and Management*, Vol. 41, n°5, p. 597-607.

Kyobe, M. (2008), “The impact of entrepreneur behaviours on the quality of e-commerce security: A comparison of urban and rural findings”, *Journal of global information technology management*, Vol. 11, n°2, p. 58-79.

Labodi, C. et Michelberger, P. (2010), “Necessity or challenge – Information Security for small and Medium Enterprises”, *Annals of the university of Petrosani, Economics*, Vol. 10, n°3, p. 207-216.

Lee, Y. et Larsen, K.R. (2009), “Threat or coping appraisal: determinants of SMB executives’ decision to adopt anti-malware software”, *European Journal of Information Systems*, Vol. 18, p. 177-187.

Litecky, C.R., Arnett, K.P. et Prabhakar, B. (2004), The paradox of soft skills versus technical skills in IS hiring, *Journal of Computer Information Systems*, Vol. 45, n°1, p. 69-76.

Longeon, R. et Archimbaud, J.L. (1999), *Guide de la sécurité des S.I. à l’usage des directeurs*, CNRS, Paris.

Loonam, J.A. et McDonagh, J. (2005), “Exploring Top Management Support for the introduction of Enterprise Information Systems: A Literature Review”, *The Irish Journal of Management*, Vol. 26, n°1, p. 163-178.

Lucas, H.C. Jr. (1981), *Implementation: the key to successful information systems*, Columbia University Press, New York.

Markus, M.L. (1983), “Power, politics, and MIS implementation”, *Communications of the ACM*, Vol. 26, n°6, p. 430-444.

Miles, M. B. et Huberman, A.M. (2003), *Analyse des données qualitatives*, De Boeck, Bruxelles.

Mitchell, R.C., Marcella, R. et 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 décision d’investissement en TIC*, in Boutary, TIC et PME : des usages aux stratégies, l’Harmattan, Paris.

Mucchielli, A. (1996), *Dictionnaire des méthodes qualitatives en sciences humaines et sociales.* Armand Colin, Paris.

Norburn, D. et Birley, S. (1988), “The top management team and corporate performance”, *Strategic Management Journal*, Vol.9, n°3, p. 225-237.

Pritchard, S. (2010). Navigating the black hole of small business security. *Infosecurity*, Sept. Oct., p. 18-21.

Ragu-Nathan, B.S., Apigian, C.H., Ragu-Nathan, T.S. et Tu, Q. (2004), A path analytic study of the effect of top management support for information systems performance, *Omega*, Vol. 32, p. 459-471.

Rainer, R.K., Marshall, T.E., Knapp, K.J. et Montgomery, G.H. (2007), "Do Information Security Professionals and Business Managers View Information Security Issues Differently?", *Information Systems Security*, n°16, p. 100-108.

Rees, J. (2010), "Information security for small and medium-sized business", *Computer Fraud & Security*, n°9, p. 18-19.

Reid, R.C. et Gilbert, A.H. (2009), "Cognitive Support for Senior Manager's Decision Making In Information Systems Security". *Proceedings of the academy of information and management sciences*, Vol. 13, n°1, p. 58-62.

Reix, R. (2004), *Systèmes d'information et management des organisations*, Vuibert, Paris.

Robinson, S. et Volonino, L. (2004), *Principles and practices of information security*, Pearson Prentice Hall, New Jersey.

Rockart, J.F. et Crescenzi, A.D. (1984), "Engaging top management in information technology", *Sloan Management Review*, Vol. 25, n°4, p. 3-16.

Ross, J. et Weill, P. (2002), "Six decisions your IT people shouldn't make", *Harvard Business Review*, November, p. 85-91.

Sanders, G.L. et Courtney, J.F. (1985), "A Field Study of Organizational Factors Influencing DSS Success", *MIS Quarterly*, Vol. 9, n°1, p. 77-93.

Schein, E.H. (1990), *Organizational culture and leadership*, Jossey-Bass, San Francisco.

Smith, S., Winchester, D., Bunker, D. et Jamieson, R. (2010), "Circuits of Power: A study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization", *MIS Quarterly*, Vol. 34, n°3, p. 463-486.

Song, J.H. (1982), "Diversification strategies and the experience of top executives of large firms", *Strategic Management Journal,* n°3, p. 377-380.

Stemberger, M.I., Manfreda, A. et Kovacic, A. (2011), "Achieving top management support with business knowledge and role of IT/IS personnel", *International Journal of Information Management*, Vol. 31, p. 428-436.

Stevens, J.M., Beyer, J.M. et Trice, M.H. (1978), "Assessing personal role and organizational predictors of managerial commitment", *Academy of Management Journal,* n°21, p. 380-396.

Vermeulen, C. et von Solms, R. (2002), "The information security management toolbox: Taking the pain out of security management", *Information Management & Computer Security,* Vol. 10, n°3, p. 119-125.

Walsham, G. (1995), "Interpretive case studies in IS research: nature and method", *European Journal of Information Systems*, n°4, p. 74-81.

Walsham, G. (2006), "Doing interpretive research", *European Journal of Information Systems*, Vol. 15, n°3, p. 320-330.

Williams, P. (2007), "Executive and board roles in information security", *Network Security*, n°8, p. 11-14.

Yin, R.K. (2008), *Case study research: design and methods*, Sage Publications, Thousand Oaks, CA.

Zwikael, O. (2008), "Top management involvement in project management: Exclusive support practices for different project scenarios", *International Journal of Managing Projects in Business*, Vol. 1, n°3, p. 387-403.

ANNEXE A : Caractéristiques des entreprises étudiées

N°	Nom générique	Structure juridique	Date de création	Dept.	Ville	Nombre de salariés		C.A. en M€
						Permanents	Temporaires	
1	Commercialisation de compléments alimentaires	S.A.	21/12/2001	34	Montpellier	15	20	3,5
2	Pépinière d'entreprises	SARL	01/07/2001	34	Montpellier	6	46 (*)	0,5
3	Conception et vente de systèmes photovoltaïques	S.A.	29/09/2000	34	Saint Mathieu	130	0	36,0
4	Conception et vente de plastiques moulés	S.A.S.	01/07/1990	34	Valergues	20	0	3,1
5	Conception et vente de peintures	S.A.S.	01/08/1988	34	Vendargues	19	0	3,0
6	Institut psychiatrique	S.A.S.	01/11/1972	34	Pignan	70	0	5,9
7	Commercialisation de produits liés au bâtiment	S.A.S.	01/01/1978	34	Vendargues	46	10	31,0
8	Travaux de charpentes et toitures	S.A.S.	01/04/1990	34	Le Crès	30	0	4,5

S.A.S : société par actions simplifiée (*) Les entrepreneurs sont comptés comme des travailleurs temporaires

N°	Code NAF	Activité
1	4791A	Vente à distance sur catalogue général
2	7022Z	Conseil pour les affaires et autres conseils de gestion
3	4669B	Commerce de gros (interentreprises) de fournitures et équipements industriels divers
4	2229B	Fabrication de produits de consommation courante en matières plastiques
5	2030Z	Fabrication de peintures, vernis, encres et mastics
6	8610Z	Activités hospitalières
7	2361Z	Fabrication d'éléments en béton pour la construction
8	4391B	Travaux de couverture par éléments

ANNEXE B : Présentation des huit cas d'entreprise

CAS DE L'ENTREPRISE 1 : Entreprise de vente par téléphone de compléments alimentaires et diététiques.

* **Implication :** Selon le dirigeant, son implication viendrait de son passé dans le secteur pharmaceutique et dans le renseignement. La notion de confidentialité est fortement mise en valeur. Il a aussi très bien compris que son entreprise vivait surtout grâce à son fichier client, et il perçoit son activité comme hautement concurrentielle. Les éléments limitant son implication sont "*que cela ne fait pas de ventes*". Son implication est perçue de manière plutôt implicite par les salariés car il n'agit pas directement ou de manière proactive vis à vis d'eux (pas d'information ou de sensibilisation), mais ils le ressentent au travers des actions mises en place. Par contre, le dirigeant est perçu comme étant à l'écoute des suggestions des salariés pour améliorer la SSI.

* **Actions :** Selon le dirigeant, il a mis en place toute l'organisation de la protection du SI de son entreprise.

"J'ai fait les définitions de fonctions, j'ai fait les définitions de postes, j'ai fait des procédures, etc. j'ai fait les rangements aussi, j'ai acheté des armoires". "C'est une impulsion, on va dire de sécurité, que j'ai mise en place". Le dirigeant dit avoir a jouer un rôle pour responsabiliser les salariés et les a sensibilisés sur les éléments critiques.

Le dirigeant déclare aussi avoir été à l'origine des mesures techniques mises en place, le système de sauvegarde notamment, en coordination avec le responsable informatique.

Il apparaît au travers des entretiens que ses connaissances en informatique sont limitées : il ne connait pas par exemple les termes "firewall" et ne sait pas quel système de sauvegarde est mis en place. Mais cela ne semble pas limiter ses actions : ce qui le bloque est avant tout le budget car il souhaiterait faire plus : en effet il est tout à fait conscient des conséquences que pourraient entrainer la perte de son fichier client (coût de reconstitution des fichiers, perte d'activité, …).

Selon le responsable informatique (appartenant à une société extérieure) les idées proviennent bien du dirigeant qui pilote la SSI de son entreprise. Lui ne relève que les dysfonctionnements. Il reconnait l'ensemble des actions mises en place par le dirigeant. Les deux salariés interrogés ont tout à fait conscience de l'importance de la continuité d'activité de l'entreprise : "*cela veut dire l'entreprise est morte si cela dure pendant deux ou trois jours*". Par contre, les deux salariés perçoivent peu l'action du dirigeant, ils n'ont pas de souvenir des sensibilisations qu'il a évoquées et pensent que cela a dû concerner d'autres salariés qui posaient problème. Un salarié se rappelle avoir signé une clause de confidentialité contractuelle, qui figure aussi dans le règlement intérieur. Donc tout a été mis en place pour que le S.I. soit protégé, même si "*c'est pas très rentable*". Le dirigeant pratique aussi un cloisonnement des informations qui circulent dans l'entreprise : "*chaque fonction doit savoir ce qu'elle a à savoir et pas forcément plus*".

CAS DE L'ENTREPRISE 2 : Pépinière d'entreprises

* **Implication :** Ce qui apparaît en premier est la faible implication de la directrice : "*je peux concevoir qu'on sécurise des informations mais je sais pas, moi je ne sécurise rien et j'ai rien à cacher".*

Sur le plan des freins, elle n'a aucune compétence technique : *"Sur les questions techniques, faut pas trop m'en poser, parce que je sais pas. Parce que ce n'est pas mon domaine, et que cela ne m'intéresse pas".* Aucun facteur positif n'a pu être identifié dans son discours.

* **Actions :** Sa passivité en termes d'actions, voire son opposition à certaines mesures de sécurité ressort aussi : pour le mot de passe *"je ne veux pas le changer parce que après sinon je l'oublie, et ça va pas. Alors j'ai demandé à ce qu'on ne le change plus".*

L'opinion du salarié qui joue le rôle de technicien est éloquente : "*sur la sécurité informatique, elle a beaucoup de mal (…) elle a des comportements dangereux dont elle ne se rend même pas compte*".

Pour lui, la direction se contente de valider le budget qu'il estime indispensable pour mettre en place des protections de base (sauvegardes). Une autre salariée, confirme qu'elle n'a reçu aucune information ni sensibilisation de la part de la directrice ou même des "salariés-techniciens".

CAS DE L'ENTREPRISE 3 : Entreprise de conception et vente de systèmes photovoltaïques.

* **Implication :** La dirigeante est plutôt impliquée *"la sécurité des informations, par rapport à la concurrence, c'est quelque chose de très-très stratégique, parce que sur 60% de notre activité, on travaille sur des montages qui sont uniques".* Mais sa vision de la SSI est parcellaire *"La sécurité informatique, pour moi c'est ce volant qui concerne plutôt la confidentialité, je dirai, ensuite les problèmes physiques".* Cette sensibilisation vient de son passé *"Je viens d'un cabinet de consulting, où tout était confidentiel".* Elle semble donc surtout concernée par l'aspect "confidentialité" de la SSI. Elle s'estime responsable, du fait de sa position dans l'entreprise. Les informations à protéger sont des montages financiers, à un niveau international.

* **Actions :** Sur le plan des actions, elle se repose surtout sur le responsable informatique, qui correspond à un poste réel du fait de la taille de l'entreprise. Elle valide les budgets, mais n'agit que très peu par elle même. Par exemple, la formation est réservée aux non-cadres *"c'est le truc que je fais sauter systématiquement".* Le manque de temps est évoqué pour justifier son comportement.

Le responsable informatique confirme que la dirigeante est très consciente des risques encourus, mais "*pour le quotidien on va dire, elle se repose entièrement sur le service informatique"*. Donc il n'y a pas vraiment de sensibilisation des salariés de la part de la dirigeante. Un des salariés confirme que seuls son chef de département et le responsable informatique assurent une certaine sensibilisation et constituent des acteurs dans la SSI. La responsable des RH n'a de contacts qu'avec le RSI. Concernant la dirigeante, "*en termes de communication, je pense qu'elle a un rôle à jouer"*, mais rien n'est réellement fait.

CAS DE L'ENTREPRISE 4 : Entreprise de conception, fabrication et vente de produits moulés en plastique

* **Implication :** Quand on lui demande les causes de son implication, elle répond "*c'est peut-être naturel*" "*cela me paraît logique*".

Toujours sur le plan de sa personnalité, elle évoque : "*il faut une certaine paranoïa, une paranoïa raisonnée".*

La directrice succède à sa mère qui lui a transmis le souci de protéger ses informations. Elle a aussi été marquée par un incident "*Nous avons eu un problème électrique, on a plus eu du tout d'informatique pendant 48 heures*", ainsi que ses conséquences *"on téléphonait à tous nos clients, à tous les gens susceptibles d'avoir appelé, pour leur signaler qu'on était en panne et pas en faillite, mais c'est assez terrifiant".*

Elle justifie les comportements de ses salariés par : *"La culture d'entreprise est liée à la fierté de travailler dans l'entreprise. (…) c'est une entreprise familiale. Et à moins d'un clash, on ne trahit pas la famille".*

* **Actions :** Elle agit beaucoup : c'est elle qui décide des actions à mettre en place, d'autant plus qu'elle joue aussi le rôle de responsable informatique : elle s'occupe des sauvegardes quotidiennes et elle est très au courant de ce qui est fait en matière de sécurité dans son entreprise : mises à jour de sécurité, antivirus, firewall, … Elle a pris un ensemble de petites mesures touchant à la protection des données de "tous les jours" : position du fax, règles concernant les documents sortants, homogénéisation du classement des documents, etc. Elle perçoit la concurrence comme très vive, c'est ce qui l'a conduite à prendre des mesures.

Mais c'est aussi elle qui sensibilise ou rappelle à l'ordre les salariés : *"Quand je vois une déviation légère, même légère, alors là, je remets la sauce, totale. Des fois qu'ils aient oublié autre chose aussi".*

Les deux salariées interrogées confirment la sensibilisation conduite par la dirigeante et le fait qu'elle soit l'interlocuteur en termes d'informatique et de sécurité des informations. La dirigeante est citée en exemple pour le broyage des documents confidentiels ainsi que pour les rappels concernant les directives ou encore les périodes durant lesquelles il faut particulièrement attention.

CAS DE L'ENTREPRISE 5 : Entreprise de fabrication et vente de peintures

* **Implication :** Le dirigeant a une forte personnalité que l'on peut qualifier de "charismatique".

"*Le risque ne me paraît pas énorme dans la mesure où on n'est pas dans des technologies de pointe (…) Il est évident qu'il faut préserver nos formules, préserver notre savoir, mais c'est pas absolument essentiel. (…) On pêche à ce niveau-là, il faut quand même faire des efforts. Cela j'en suis convaincu.*"

"*La perte de disponibilité serait beaucoup plus grave. On est dépendants de l'informatique, mais il nous est arrivé d'avoir des pannes informatiques, qui ont duré, on a survécu… (…) On a un contrat d'assistance et de maintenance, mais bon, après un certain délai*". Il relativise toutefois : *"si l'informatique tombe en panne et qu'on ne peut plus enregistrer les commandes avec l'ordinateur, on le fera à la main".*

La concurrence est perçue comme étant très vive mais le risque de se faire voler le fichier clients est considéré comme nul, car les concurrents connaissent leurs clients. Les formulations des peintures élaborées sont secrètes, mais il est assez facile de les analyser une fois commercialisées.

Il se considère comme impliqué "*l'implication, ah ça oui, je suis impliqué, mais cela se traduit par pas grand-chose*". Il reconnait un manque de compétences en informatique.

* **Actions :** L'entreprise étant "familiale", le dirigeant ne sensibilise pas ses salariés, il considère que tous leurs comportement doivent respecter un "contrat moral". Le dirigeant est d'un naturel suspicieux : *"il est hors de question que l'on fasse de la télémaintenance, si vous faites ça, vous dégagez".*

Un des éléments bloquants pour mettre en place une sécurité satisfaisante est que "*si on veut vraiment protéger notre fonds de commerce, il faut repenser complètement notre organisation".*

Il sort les bandes de sauvegarde de l'entreprise régulièrement.

Un des salariés, le responsable qualité, a pris en charge l'informatique et la protection du S.I. Il partage les mêmes craintes que le dirigeant concernant la société extérieure de maintenance informatique.

Un autre salarié s'exprime comme le dirigeant. "*Et tout ça ne doit pas être divulgué, c'est tout. C'est un fait*". "*C'est un non-dit, on n'a pas besoin que ce soit dit pour le faire*".

Une autre salariée dit souvent "on", ce qui conforte cette impression de culture partagée de SSI. Suite à une perte de données "*il a fallu refaire le travail de plusieurs jours, et à la suite de quoi, je pense que c'est là qu'on a compris qu'il fallait faire une sauvegarde tous les jours*".

CAS DE L'ENTREPRISE 6 : Etablissement de santé (institut psychiatrique)

* **Implication :** Son implication est très limitée : *"On est sensibilisés par rapport au secret médical et au secret professionnel de manière générale". "C'est moi qui suis responsable (…) de la "sécurité au sens large", mais "sur un plan plus informatique on n'a personne de spécifique"*. Elle ne donne pas vraiment de facteurs d'implication : *"Peut-être que ça m'est personnel, mais je crois que cela fait partie de la culture maison"*.

* **Actions :** Quand on lui parle de ses actions en termes de SSI : *"dans ce domaine là, il n'y a pas de stratégie vraiment bien définie, on gère plus en fonction des contraintes normatives, cela nous laisse peu de marge de manœuvre budgétaire pour investir (…) de notre propre initiative"*. Elle souligne son manque de connaissances : *"Ça, je ne sais pas, en plus je ne m'y connais pas en informatique. Elle n'a a*ucune réflexion sur la continuité d'activité des serveurs, et quand il y a un problème *: "j'appelle notre prestataire informatique"*.

Elle reconnait certaines actions : *"On a informatisé les prescriptions", "On a mis en place un nouveau serveur avec 2 disques durs et une sauvegarde",* mais encore une fois cela ne fait que répondre aux impératifs des normes du domaine.

"Sur la confidentialité des informations concernant les personnes, cela fait partie de leur contrat de travail. Il y figure la notion que tout salarié est tenu au respect de la confidentialité. Sachant ensuite que pour les médecins et les infirmières, cela fait partie de leur fonction même, que de respecter le secret professionnel. (…) On les sensibilisera moins par exemple, sur la sécurité informatique. Donc, on est très focalisés sur ce qui est données liées aux patients."

Mise à part cette sécurité liée au dossier médical, rien n'est fait : mots de passe de 5 voire 2 caractères et jamais changés, sauvegardes très rares des postes des salariés. Les sauvegardes importantes ne sont réalisées que toutes les semaines.

Il y a des communications orales, notes de service, réunions, mais pas vraiment sur la sécurité des informations. Elle évoque le manque de budget comme un frein.

D'après un salarié : Le prestataire extérieur, la directrice et l'attachée de direction "*sont quand même un peu les pivots*".

La direction apporte un soutien. Mais selon une autre salariée, aucune sensibilisation à la sécurité des informations n'est réalisée, autre que celle liée au secret médical.

CAS DE L'ENTREPRISE 7 : Exploitation de carrières, fabrication et commercialisation de produits liés au BTP

* **Implication :** Pour elle, la sécurité se résume à : *"Cela concerne la discrétion de chaque personne"*. Lorsque l'on parle de perte d'informations : "*s'il fallait rattraper une semaine de travail, on serait déjà mal"*, et elle redoute un problème sur *"la saisie des bons de livraison, quand cela se transforme en facture. Là, ce serait la catastrophe*". Enfin, elle craint l'incendie et le vol de dossiers.

* **Actions :** Quelques actions ont été mises en place : elle prend chez elle la bande de sauvegarde chaque jour, mais l'antériorité n'est que d'une seule semaine. Elle a demandé des mots de passe. Il n'y a personne qui s'occupe de la SSI à part elle, un prestataire extérieur la prévient des dangers et décide de l'évolution des matériels et protections.

Son avis sur les salariés : *"il y a une telle masse de travail pour chaque personne que si elle s'amuse (...) à y passer des heures, avec ce qu'elle doit faire à côté, il faudrait qu'elle reste jusqu'à 11 heures du soir". "Pour les informations sur les postes de travail chacun se débrouille"*.

Les salariés n'ont reçu aucune formation ni sensibilisation à la sécurité. Une salariée est assez préoccupée de la confidentialité des informations du fait de son poste (R.H.), elle fait ses sauvegardes. Un autre salarié ne fait absolument rien et rejette la faute sur la direction qui ne lui donne pas les moyens.

CAS DE L'ENTREPRISE 8 : Fabrication et commercialisation de charpentes et toitures

* **Implication :** Il reconnait qu'il s'implique très peu, qu'ils sont en retard en termes de SSI, mais rien n'est fait même si *"on devrait en faire beaucoup plus"*. Pourtant, il est conscient des risques encourus, puisqu'il reconnait qu'un blocage durant plus d'un jour poserait des problèmes. Lorsque l'on parle d'un possible incident : *"Ça gênerait énormément tout ce qui est paie, tout ce qui est comptabilité et secrétariat, tout le monde à la limite, sauf moi ". Mais "on est toujours passés au* travers".

L'informatique et a fortiori la SSI le dépassent *"et en plus j'aime pas l'informatique"*.

* **Actions :** Le dirigeant justifie son manque d'action par d'autres priorités et le manque de budget. Non seulement il n'agit pas mais a même demandé à ce que les mots de passe soient enlevés car cela était gênant.

Un salarié (un dessinateur), a pris la fonction de responsable informatique/SSI. Il a appris sur le tas : *"En gros j'ai appris l'informatique pour pouvoir me passer des informaticiens, pour être peinard"*. Son jugement du directeur : *"Non il s'investit pas … je ne fais pas ce que je veux, je n'ai pas le budget que je veux pour faire ce que je veux."*. *"Un PC, de toute façon, il en voit l'utilité directe alors qu'un serveur il ne le voit pas"*. *"Est-ce que la démarche vient de la tête de l'entreprise ? Non, pas du tout !"*. Il donne l'impression de lutter seul, sans appui de la direction, et n'a pas de prise sur les autres salariés *"L'utilisateur par exemple, il oublie à peu près une fois par semaine de faire ses sauvegardes hebdomadaires"*.

Un seul salarié parle de recommandations de confidentialité et de broyage des documents de la part du dirigeant. Sinon Aucun salarié n'a reçu de sensibilisation ou formation. La sécurité apparaît comme très faible : aucun mot de passe, les sauvegardes ne sont pas faites. Le dirigeant semble toutefois avoir une influence sur lui *"par respect, je garde la confidentialité"*, il évoque aussi sa "*loyauté à l'entreprise"*.

ANNEXE C : Les facteurs de l'implication et l'action des dirigeants

	Entreprise 1	Entreprise 2	Entreprise 3	Entreprise 4
Données signalétiques	51 ans Homme Bac+5	42 ans Femme Bac+5	32 ans Femme Bac+5	31 ans Femme Bac+2
Taille entreprise	15 + 20 temporaires	6 + 46 temporaires	130	20
Eléments personnels	Passé dans la pharmacie, "renseignement" dans l'armée	Rien d'évoqué	Passé : confidentialité dans cabinet de consulting "*C'est par tempérament*"	C'est logique – naturel Succède à sa mère qui lui a transmis ses priorités
Eléments de contexte	Concurrence très forte. Fichier clients 'vital'. A estimé la valeur de ses informations	Rien d'évoqué	Sécurité très stratégique Des salariés ont porté atteinte aux informations Secrets industriels à protéger	Effet "vaccin" : son entreprise a été bloquée 2 j Culture d'entreprise-famille
Niveau de connaissances	"*Je n'y connais pas grand-chose*".	"*Je sais pas, ce n'est pas mon domaine et cela ne m'intéresse pas*". "*Je ne suis pas compétente et puis j'ai pas envie de l'être*"	Satisfaisant	Satisfaisant
Ressources (temps – argent)	"*Le coffre anti-incendie, j'ai eu ça dans le passé, cela coûte la peau des fesses*" "*On le fera dès qu'on aura trois sous*".	Non évoqué	"*On a effectivement prévu de la déployer, mais on a eu pas mal de projets qui ont été jugés prioritaires et sur le coup c'est passé un petit peu au second plan*" : plusieurs mois de perdus. Pas le temps d'assister aux formations.	Non évoqué, ne semble pas être un problème.
Autres éléments négatifs	"*C'est de l'énergie qui n'est pas productrice de ventes, et dans une petite boîte c'est dur*". N'a pas confiance dans ses salariés : segmente les informations	"*J'ai rien à cacher*" Le risque que son entreprise disparaisse ne la gêne pas. Est contre les mots de passe.	Vision trop limitée à la confidentialité. N'a pas chiffré les sinistres possibles : "*Il y a tellement de cas de figure différents*".	On n'est pas "secret-défense" non plus.
Avis sur l'implication	Se dit impliqué, le RSI confirme, les salariés partiellement. **Implication : forte.**	Se dit non impliquée, confirmation par tous les acteurs de ceci. **Implication : non impliquée.**	Se dit impliquée, confirmé par le RSI et ses collaborateurs proches. **Implication : moyen+**	Se dit impliquée, confirmé par les salariés. **Implication : forte**.
Avis sur le niveau d'action	Il a mis en place un grand nombre de mesures de sécurité qu'il qualifie "*d'artisanales*". **Action : forte.**	Elle n'a fait qu'expliquer ce qu'elle voulait mais ne suit pas l'avancement. Elle se repose sur les deux salariés qui agissent pour préserver un minimum de sécurité. Ils reconnaissent des comportements dangereux de sa part. **Inaction.**	Elle se repose entièrement sur le RSI. Le RSI confirme son discours. Ses informations : "*j'y fais très attention*" et la gestion du RSI sont ses seules actions. **Action : moyenne à faible.**	Elle dit s'occuper de tout. Elle s'assure que les consignes sont respectées et rappelle à l'ordre les salariés sinon. Les salariés confirment ceci. **Action : forte.**

	Entreprise 5	Entreprise 6	Entreprise 7	Entreprise 8
Données signalétiques	55 ans Homme Autodidacte Ancienneté de 35 ans	35 ans Femme Bac+5	50 ans Femme Bac+2 Ancienneté de 27 ans	43 Homme Autodidacte
Taille entreprise	19	70	46	30
Eléments personnels	Attachement à son entreprise familiale.	"*Peut-être que ça m'est personnel*"	Rien d'évoqué	Rien d'évoqué
Eléments de contexte	Craintes vis-à-vis du prestataire informatique, pas de confiance.	Evoque le secret médical et les accréditations "*C'est surtout se protéger de l'extérieur*"	Les prix sont à cacher, elle craint l'incendie et le vol de dossiers. "*s'il fallait rattraper une semaine de travail, on serait déjà mal*"	"*Ça gênerait énormément tout ce qui est paie, tout ce qui est comptabilité et secrétariat, tout le monde à la limite, sauf moi* "
Niveau de connaissances	Manque de connaissances.	"*Je ne m'y connais pas en informatique*"	Connaissances moyennes	"*J'aime pas l'informatique*"
Ressources (temps –argent)	"*Il faut changer notre façon de travailler ... repenser complètement notre organisation*"	Suivi des normes du secteur médical : peu de marge de manœuvre budgétaire pour la sécurité. "*On suit plus les textes qu'autre chose*".	Le budget doit être justifié par la société extérieure.	Le budget Il y a d'autres priorités.
Autres	"*Le risque ne me paraît pas énorme dans la mesure où on n'est pas dans des technologies de pointe*" On a eu "*des pannes informatiques, qui ont duré, on a survécu*". Pour les clauses écrites ou procédures : "*Quel est l'intérêt ?*". Tout est basé sur la confiance : "*Le contrat, il est moral*".	Aucun sinistre n'a été rencontré.	Pas de sinistre particulier.	Bloque les décisions du salarié concernant les mots de passe et l'achat d'un serveur. Concernant les sinistres : "*On n'a pas de soucis*", "*on est toujours passés au travers*"
Avis sur l'implication	Se dit impliqué. **Implication : moyen+**	Se dit sensibilisée, mais au secret médical, la confidentialité. **Peu impliquée** dans les faits (retours des salariés).	Se dit impliquée, non confirmé par les salariés. **Implication : moyen+**	Se dit **très peu impliqué.** Un salarié a reçu des consignes pour broyer les documents.
Avis sur le niveau d'action	Reconnait agir peu et laisse agir un salarié. **Action : faible.**	**Action moyenne**, uniquement conformément aux normes. Laisse-faire un extérieur. Pas d'homogénéité.	Agit, mais doit se reposer sur la société extérieure. **Action : moyenne.**	**Aucune action**, le salarié qui s'occupe de l'informatique lutte pour avoir des moyens.

ANNEXE D : Les salariés-RSSI, une prise en charge informelle.

	Entreprise 2	**Entreprise 5**	**Entreprise 8**
Fonction	Conseiller en création d'entreprise	Responsable qualité	Dessinateur industriel
Connaissances	*Je n'ai pas l'expertise technique pour valider la démarche du prestataire.* *J'ai un niveau vraiment moyen en informatique, je n'avais pas du tout d'expertise, ça ne m'a pas aidé à rationaliser une situation avec un prestataire défaillant.*	*Sans vouloir me mettre en valeur, je sais un peu plus de choses, ce qui est normal, la génération d'après en sait encore plus.* *Ça, je peux le faire, si c'est pas trop compliqué.*	*Donc en général je sais faire, mais ça dépend du temps que j'ai, selon le temps que j'ai de dispo et l'envie aussi, je répare moi-même. Sinon j'appelle notre société extérieure.*
Motivations avancées	*On a perdu tous, des données que ce soit personnelles ou professionnelles depuis plusieurs années, donc **on sait ce que ça représente, c'est une préoccupation constante** et à la limite paranoïaque ! Cela représente pour moi **la pérennité et l'intégrité de l'outil de travail**. On s'en est rendu compte après en avoir perdu une partie.*	*Moi je parle parce que **je suis le plus jeune rentré**, par rapport à une autre génération qui est ici, **j'ai quand même pratiqué l'informatique plus que les autres ne l'ont fait.***	*Ça vient de moi parce que je connais le problème, j'ai déjà perdu des données, pas spécialement ici, mais enfin des programmes. [Le prestataire] mettait toujours vachement de temps à intervenir, donc en gros **j'ai appris l'informatique pour pouvoir me passer des informaticiens, pour être peinard.***
Relations avec le dirigeant	*Sur la sécurité des informations, elle sait ce qu'il faut dire, ce qu'il ne faut pas dire. Là-dessus, c'est elle qui nous cadre. Par contre, **sur la sécurité informatique, elle a beaucoup de mal donc, avec l'outil lui-même, elle sait pas, elle a des comportements dangereux dont elle ne se rend même pas compte**. Et, quand je lui explique, ça passe à la trappe assez systématiquement quoi. Donc je dois contrôler son poste ...* *Si je fais pas les antivirus pour elle, elle ne le fera pas spontanément, je lui dis qu'il faut qu'elle fasse les mises à jours quand une petite fenêtre lui dit "mises à jours Windows", mais elle le fait pas. Elle a des habitudes comme ça qui sont pas faciles à faire évoluer quoi.*	[Je joue le rôle de responsable sécurité], *mais **sous l'avis de M. xx. Je rapporte ce qu'il y a à M. xx, et il me dit "bon, il faut contacter notre société informatique"**, qui viendra et m'aidera à faire une réparation ou réparer un logiciel antivirus qui ne se met pas à jour tout seul, voilà, c'est ça.* *Je pense qu'on me surveillait au début, cela je pense que M. xx vous le dira, c'est sûr qu'ici on regarde si les gens sont dignes de confiance.* [Réponse à de nombreuses questions] *"Ça, c'est M. xx qui pourra vous répondre" ou "Il faut voir avec M. xx pour cela".*	*Si la démarche vient de la tête de l'entreprise ? Non, pas du tout ! Ça vient de moi. **Il s'investit pas, je n'ai pas le budget que je veux pour faire ce que je veux.*** [centralisation des sauvegardes] *Je vous dis pas comment **je dois batailler** pour acheter rien qu'un PC. Un PC, de toute façon, il en voit l'utilité directe, alors qu'un serveur il ne la voit pas, donc. Pour lui, même 1000 €, c'est quand même une grosse somme. Donc...* *Le patron ne fait jamais ses sauvegardes, je lui fais un coup de temps en temps. Mais il ne les fera jamais, faut pas que je me leurre. [...] Le patron n'est pas prêt à accepter d'avoir un mot de passe.*
Relations avec les employés	*Je pense que les gens réagissent à partir du moment où ils ont un problème, quand ils ont pas de problème, ils vont pas spontanément prendre des mesures de prévention [...]. **Faudrait aller vérifier qui c'est qui a regardé les vers depuis la dernière fois que je l'ai fait. Il n'y a pas grand monde qui l'a fait.*** *Je crois que plus on automatise et moins on en demande aux utilisateurs, mieux c'est, et en même temps, c'est pas leur boulot.* *Il y avait toujours un truc qui faisait que l'informatique marchait pas, et à peu près sur tous les postes. Donc **on n'a pas eu de période où les utilisateurs pouvaient disposer de postes fiables. Donc, demander à quelqu'un de mettre en place des procédures, ou de suivre des protocoles pour la fiabilité informatique, c'est un peu des foutaises quoi**. Pour l'utilisateur qui n'est pas convaincu par l'informatique et qui s'en sert juste comme outil, il va se dire "on se fout de moi".*	*Au niveau salarié, il n'y a que le dirigeant, le responsable production, moi-même, le comptable et la secrétaire, qui font de l'informatique. Mais bon la secrétaire utilise toujours le même logiciel et l'informatique, elle ne connaît pas trop.* *La comptable avait perdu quelques informations, alors j'ai remonté les informations.* *Enfin, les gens sont là depuis longtemps, donc il y a une certaine confiance, mais au niveau salarié, je ne vois pas quelqu'un qui puisse aller voir dans le système et en profiter.* ***On a un serveur et puis on a des sauvegardes journalières, et tous les soirs j'emporte la bande**. Pour leurs données, il y a des clés ou des choses comme ça, pour que ce soit sauvegardé plus rapidement.*	***J'ai recommandé à la comptable de faire des sauvegardes**. On a mis en place un truc, mais ça lui convient pas trop. **La comptable je lui fais ses sauvegardes une fois par semaine.*** *Chacun est responsable de ses sauvegardes. **J'ai essayé de faire ce qu'il faut pour que les gens fassent leurs sauvegardes mais j'ai pas envie de me mettre à les faire à leur place surtout qu'à la limite l'informatique c'est pas mon boulot d'origine.*** *L'utilisateur par exemple, oublie à peu près 1 fois par semaine de faire ses sauvegardes hebdomadaires. Donc, si je lui dis pas de le faire il ne le fera pas, plus par manque de temps que par mauvaise volonté. Personne n'est vraiment de mauvaise volonté.* ***J'essaye de responsabiliser chacun, et puis après, s'il se passe quelque chose, on verra bien ce qu'il se passe**...*
Autres problèmes globaux rencontrés	***On mesure le risque, et on n'arrive malgré tout pas à s'en prémunir complètement.*** *Cela représente aussi un casse-tête pour moi. **Le problème, c'est que je peux pas évaluer l'erreur, qui l'a faite et d'où elle vient.*** *C'est un cauchemar ! Même ceux qui trouvent un intérêt à l'informatique n'y arrivent pas, à sécuriser tous ces trucs.*	***On craint que notre société informatique soit malhonnête** et s'ils veulent, puisqu'ils font des interventions sur l'informatique, ils ont tous les droits d'accès, eux savent beaucoup plus que moi. Maintenant, il faut faire confiance à quelqu'un, alors...* *Au niveau des protections extérieures, on a les firewalls qui doivent normalement empêcher les extérieurs d'entrer, normalement, je dis bien...*	*Je fais ma sauvegarde sur DVD et donc c'est vrai, ça me prend vite ½h dans la semaine, et j'essaye de le faire qu'une fois par semaine en espérant que ça suffit.*

AUTEURS

Yves BARLETTE est professeur associé au Groupe Sup de Co, Montpellier Business School, depuis 1989. Il enseigne les systèmes d'information et la sécurité de l'information dans son institution ainsi qu'à l'IAE de Montpellier II. Il a obtenu sa thèse en 2006 et il est membre du MRM (Montpellier Research in Management). Ses recherches sont consacrées depuis l'année 2000 à la sécurité de l'information, plus particulièrement aux aspects comportementaux des acteurs des organisations.

Adresse : Montpellier Business School, 2300 Avenue des Moulins 34185 Montpellier

Mail : y.barlette@supco-montpellier.fr

Marie-Laurence CARON-FASAN est maître de conférences à l'IAE de Grenoble et membre du laboratoire du CERAG UMS CNRS 5820 de l'Université Pierre Mendès France de Grenoble. Ses recherches portent sur la veille stratégique, l'anticipation et les signaux faibles. Elle a publié deux livres et plusieurs articles dans des revues françaises et européennes sur ce sujet.

Adresse : Université Pierre Mendes France, IAE de Grenoble, BP 47, 38040 Grenoble

Mail : mcaron@upmf-grenoble.fr

Sabine CARTON est maitre de conférences à l'IAE de Grenoble, université Pierre Mendès-France et membre du CERAG (UMR 5820). Ses travaux portent essentiellement sur le rôle de la culture dans le domaine des S.I., sur l'adoption de T.I (pré adoption) dans une perspective institutionnaliste, ainsi que sur les relations au sein des équipes de projet S.I.

Adresse : Université Pierre Mendes France, IAE de Grenoble, BP 47, 38040 Grenoble

Mail : sabine.carton@iae-grenoble.fr

Armelle FARASTIER est enseignant-chercheur, maitre de conférences, à l'IAE de Grenoble, université Pierre Mendés France. Ses travaux portent plus particulièrement sur la gestion des connaissances au sein des organisations, la gestion de projets en SI, l'approche processus.

Adresse : Université Pierre Mendes France, IAE de Grenoble, BP 47, 38040 Grenoble

Mail : armelle.farastier@iae-grenoble.fr

Cécile GODE est actuellement chercheur au Centre de Recherche de l'Armée de l'Air (CReA) en charge de l'équipe travaillant sur le management des organisations de défense. Elle est aussi associée au laboratoire GREDEG UMR 7321 CNRS. Ses recherches portent sur les systèmes d'information et le management stratégique ainsi que sur les processus de coordination et de décision en environnement extrême.

Adresse : Centre de Recherche de l'Armée de l'Air (CReA) 10401 – BA 701 – 13661 Salon air

Mail : cecile.gode@inet.air.defence.gouv.fr

Valérie HAUCH est Maître de Conférences à l'Université de Nice-Sophia Antipolis. Membre du GREDEG UMR 7321 CNRS, elle mène des recherches sur les liens entre innovation, créativité et communication, en particulier dans le contexte des réseaux et territoires.

Adresse : Université de Nice Sophia Antipolis

Mail : hauch@unice.fr

Mélanie LASOU est lieutenant, officier-élève de la promotion 2009 de l'Ecole Militaire de l'Armée de l'air.

Adresse : Ecole Militaire de l'Armée de l'air

Mail : elanie.lasou@inet.air.defense.gouv.fr

Jean-Fabrice LEBRATY est professeur de Sciences de Gestion à l'Université de Lyon3 / IAE. Il est membre du laboratoire de recherche Magellan EA3713 et associé au GREDEG UMR 7321. Spécialisé en gestion des systèmes d'information et de communication, ses recherches portent notamment sur la prise de décision et sur les relations entre foule et technologie de l'information.

Adresse : Université de Lyon 3

Mail : jean-fabrice.lebraty@univ-lyon3.fr