Une étude des comportements liés à la sécurité des systèmes d'information en PME

Yves BARLETTE

Docteur en Sciences de Gestion, Professeur Associé,
Groupe Sup de Co Montpellier – CEROM

RÉSUMÉ

Peu de travaux scientifiques ont cherché à appréhender la dimension organisationnelle de la sécurité des SI (SSI). Après une revue de la littérature qui met en évidence les lacunes de ce domaine, nous discutons de l'adaptation de modèles consacrés à d'autres domaines, tels que les comportements d'acceptation et/ou d'utilisation des TIC ou encore des théories tirées de la psychologie ou la criminologie. Ceci permet d'aboutir à un cadre conceptuel et à trois propositions de recherche concernant les dirigeants et salariés. Une étude qualitative a permis de confirmer ces propositions et fait apparaître la spécificité des comportements liés à la SSI. Elle met notamment en évidence un phénomène de compensation, dans le cas où le dirigeant est faiblement impliqué dans la SSI de son entreprise, qui correspond à la prise en charge de la SSI par un salarié, et ce de manière informelle.

Mots-clés : Sécurité, Information, Comportement, Motivation.

ABSTRACT

Many studies exist on the technical aspects of Information System's security, but organizational issues have been neglected. After a literature review that highlights the weaknesses in this particular field, we examine I.T. acceptation and adoption models and other fields such as psychology and behavioural theories. The conceptual framework thus constituted has led us to 3 research propositions. A qualitative methodology was conducted in 9 SMEs, where 30 semi-structured interviews found support for these propositions. This research corroborates the specificity of security behaviours and highlights compensation phenomena in case of managers' low implication and more particularly the informal employee's assumption of the responsibility of "chief information security officer".

Key-words: Security, Information, Behaviour, Motivation.

INTRODUCTION

L'essor semble-t-il inexorable des technologies de l'information au sein des organisations fait que les questions relatives à la sécurité des systèmes d'information (SSI) représentent des problèmes grandissants : en effet, depuis 1999, en dépit de systèmes de protection de plus en plus sophistiqués (parefeux, antivirus, anti-spywares, etc.) la croissance moyenne des vulnérabilités déclarées par les entreprises est supérieure à 40 % par an (CERT, 2007). Ce constat nous amène à considérer que les problèmes des entreprises résident ailleurs que dans de simples progrès technologiques. Au niveau de la recherche académique, la question de la SSI soulève de nombreux intérêts, car des lacunes existent tant sur le plan de l'élaboration de théories (Dhillon et Backhouse, 2001) qu'en matière de recherches empiriques (Kotulic et Clark, 2004). La problématique de la SSI a trouvé de nombreuses propositions sur des aspects techniques, mais peu de travaux scientifiques ont cherché à en appréhender la dimension humaine. La littérature en Sciences de Gestion insiste pourtant depuis longtemps sur le fait que les salariés représentent souvent un maillon faible (Adams et Sasse, 1999) face auquel les problèmes d'ordre purement technique ne doivent pas servir d'échappatoire (Davenport, 2002). La sécurité gagne ainsi à être considérée comme un problème de gestionnaires et non de techniciens (Reix, 2004), devant 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). Dans cette quête, l'objectif de cet article est d'appréhender les comportements relatifs à la sécurité des SI des acteurs au sein des entreprises et, en cela, de resituer la problématique de la sécurité des systèmes d'information sous une dimension organisationnelle.

Cette étude sera ciblée sur les PME, tout d'abord parce qu'en France, selon l'INSEE, (2006), parmi les entreprises de plus de 10 salariés, plus de 97 % des entreprises comptent moins de 250 salariés. Ensuite, parce que dans les enquêtes portant sur la SSI, ce sont les PME qui présentent les plus grandes divergences entre les protections mises en place et la fréquence des sinistres, de plus elles accusent un retard important sur de plus grandes entreprises (Clusif, 2004). Deuxièmement, une étude de la littérature académique montre que les PME font face à des problèmes plus importants que ceux rencontrés par des entreprises de plus grande taille : elles ont des problèmes de recrutement de personnes qualifiées dans les technologies de l'information et de la communication (TIC) (Monnoyer, 2003) et elles rencontrent plus de problèmes dans l'appréciation des risques encourus (Gupta et Hammond, 2005). Il apparaît aussi un manque global de sensibilisation à la SSI (Mitchell *et al.*, 1999). Les PME présentent donc des spécificités vis-à-vis de la SSI qui justifient une meilleure compréhension des problématiques et comportements associés. Au niveau des acteurs étudiés, nous avons choisi de nous focaliser sur les dirigeants et les salariés. Le rôle du responsable informatique a été examiné mais sera peu traité dans cette contribution, car il comporte une forte part d'aspects technologiques, de plus ce poste s'est

avéré rare dans les entreprises étudiées.

Les trois éléments que nous venons d'examiner, dimension organisationnelle de la SSI, comportement des acteurs, et la taille de l'entreprise, conduisent à cette question de recherche : « **quels sont les déterminants des comportements liés à la sécurité des systèmes d'information dans les PME ?** ». Pour répondre à cette question, en première partie de cet article, l'analyse de la littérature a pour objectif d'apporter un éclairage sur les comportements relatifs à la SSI des salariés et des dirigeants. Il ressort principalement de cette analyse que l'implication et la participation du dirigeant jouent un rôle majeur dans la sécurité du SI de son l'entreprise. Au sujet des comportements des salariés relatifs à la SSI, la littérature étant peu développée, nous avons ouvert nos investigations à des modèles touchant à des comportements plus larges, tels que les comportements d'acceptation ou d'utilisation des SI. Nous avons discuté de la pertinence de l'utilisation des construits de ces modèles et de leur adaptation dans le cadre de la compréhension des comportements relatifs à la sécurité des SI.

La seconde partie de cet article présente les résultats d'une étude empirique conduite auprès de neuf PME appartenant à des secteurs variés, tels que la commercialisation de produits diététiques, la fabrication de peintures, l'exploitation de carrières, etc.

Les 30 entretiens semi-directifs conduits systématiquement auprès des directeurs, de cadres ou de simples employés de ces entreprises ont apporté quatre enseignements principaux :

1. il existe effectivement un lien entre le niveau de sécurité mesuré et le niveau de l'implication du décideur dans la SSI ;
2. l'implication des salariés dans la SSI est principalement liée à certains facteurs personnels, tels que les convictions personnelles ou l'attachement à l'entreprise et dépend aussi dans une certaine mesure de l'implication du dirigeant ;
3. l'identification des dispositifs qui peuvent être mis en place, afin d'améliorer le niveau de sécurité de l'entreprise, ainsi que les possibilités de les adapter afin de les rendre plus efficients ;
4. l'identification d'un phénomène d'auto-organisation conduisant à un rééquilibrage du niveau de sécurité de la PME, quand le dirigeant n'est pas ou peu impliqué : ce phénomène n'avait pas été prévu car il n'avait pu être décelé dans l'analyse de la littérature.

En conclusion, cet article présente les pistes de recherche ouvertes par cette investigation, notamment le fait que le phénomène de rééquilibrage et l'influence des dirigeants sur les salariés doivent être étudiés de manière plus approfondie.

1. REVUE DE LA LITTÉRATURE ET CADRE D'ANALYSE

1.1. Le comportement des acteurs relatif à la SSI

Si l'on considère que la sécurité du système d'information réside moins

dans l'édiction de règles de bonnes pratiques (« penser à faire régulièrement des sauvegardes », « ne pas communiquer ses mots de passe à des tiers », etc.) que dans l'introversion des conduites correspondantes par les différents acteurs de l'organisation (employés, managers, dirigeants, etc.), alors il convient d'appréhender notre sujet sous l'angle des théories des comportements telles qu'utilisées en Sciences de Gestion.

De nombreuses théories ont été examinées, nous n'avons retenu ici que les plus pertinentes dans le cadre de notre étude. Ces théories peuvent être regroupées en quatre grandes familles, chacune apportant un élément de compréhension des comportements relatifs à la SSI.

Le premier volet est constitué de trois théories « comportementalistes », qui ont été d'abord été utilisées dans le domaine des TIC pour mieux comprendre l'adoption et l'utilisation des technologies (Davis *et al.*, 1989 ; Davis *et al.*, 1992).

La première est **la théorie de l'action raisonnée (TRA)** (Ajzen et Fishbein, 1980) qui postule que l'intention découle de l'attitude et des normes subjectives, et va conditionner le comportement. Il a été reproché à cette théorie de ne pas inclure la difficulté que peut présenter un comportement « technique », c'est pourquoi **la théorie de prévision du comportement (TPB)**, a rajouté à la TRA la maîtrise perçue du comportement (Ajzen, 1991). Les construit utilisés dans ces deux théories paraissent adaptables au contexte des comportements relatifs à la SSI, que ce soit l'attitude vis-à-vis d'un comportement ou les normes subjectives (i.e. l'influence des autres, comme par exemple « pirater, cela n'est pas bien »). De même, la maîtrise perçue peut être prise en compte dans un comportement en SSI qui inclurait des aspects « techniques » comme par exemple les manipulations à effectuer pour « faire ses sauvegardes ».

Un comportement en SSI peut apporter des bénéfices personnels (protection de ses informations) ou externes (reconnaissance d'autrui pour la protection des informations), mais les deux modèles précédents ne prennent pas suffisamment en compte ces conséquences positives. C'est pourquoi nous avons étudié **le modèle de la motivation (MM)** extrinsèque, (Davis *et al.*, 1992), ou intrinsèque (Deci et Ryan, 1985), s'intéressant aux bénéfices apportés par l'adoption et l'utilisation des TIC.

Le deuxième volet correspond à un modèle que nous avons retenu car certains comportements en SSI incluent des aspects techniques : **le modèle d'acceptation de la technologie (TAM)** dérive de la TRA et a été adapté afin de prédire l'acceptation et l'utilisation des TIC (Davis, 1989 ; Davis *et al.*, 1989). Il est basé sur l'utilité et la facilité d'utilisation perçues. Si la facilité d'utilisation peut effectivement être rapprochée d'un comportement en SSI, la « mesure ou l'estimation » de l'utilité perçue d'un comportement relatif à la sécurité semble s'en écarter. En effet, limiter les risques de l'occurrence d'un problème et de ses conséquences revient à mener des actions dont la perception de l'utilité ne pourra pas être réduite à des indicateurs

comme la productivité, la facilité d'utilisation, etc[1].

Certains comportements liés à la SSI peuvent soit mettre en danger la vie de l'entreprise, soit être tout simplement illégaux ; afin de prendre en compte ceci, notre troisième volet correspond à deux théories tirées de la psychologie et la criminologie. **La théorie des liens sociaux,** (Gottfredson et Hirschi, 1990 ; Jenkins, 1997), postule qu'une personne adopte un comportement délinquant quand l'insuffisance de liens sociaux lui en laisse la liberté. La théorie est basée sur quatre construits qui sont réutilisables dans le contexte de la SSI: l'attachement à l'entreprise (qui pourrait expliquer des comportements pour préserver son entreprise), le sens du devoir (une responsabilité en SSI plus grande), l'implication dans le travail (qui évite de « mauvaises actions »[2], comme prendre des risques en surfant sur des sites sensibles), les croyances dans les normes et l'autorité (pour respecter une charte de SSI par exemple). Mais cette théorie n'inclut pas les sanctions éventuelles pour les fautes commises, ce qui est pris en compte dans la **théorie générale de la dissuasion** (General Deterrence Theory). Elle résulte de l'adaptation au domaine de la SSI de théories liées à la criminologie (Straub et Welke, 1998). Les individus ayant l'intention de commettre des actions incorrectes peuvent en être dissuadés s'ils sont convaincus que la probabilité d'être pris et sévèrement punis est quasiment certaine. C'est d'ailleurs la seule qui ait été élaborée spécifiquement dans le domaine de la SSI.

Le quatrième volet correspond à des théories qui complètent celles vues dans le volet précédent en abordant des problématiques liées à la morale et à l'éthique. Le modèle des **codes d'éthique** de Harrington (1996) a permis d'étudier l'effet des codes d'éthique sur l'intention et l'opinion des employés, relatives à la bonne utilisation des ordinateurs. Même si leurs effets sont limités, variables selon les personnes et concernent certaines pratiques seulement, des décideurs impliqués peuvent les renforcer par des rappels et ainsi augmenter leur influence sur les comportements. Pour Harrington, (1996), les décideurs doivent agir sur le climat moral de l'entreprise et guider les employés dans le sens désiré. La théorie des **domaines de développement moral** complète le modèle précédent car elle prend mieux en compte l'influence de la moralité sur les comportements (Gattiker et Kelley, 1999).

Le tableau 1 ci-après résume les théories retenues et les construits qui les caractérisent.

Du fait du peu de travaux portant spécifiquement sur les comportements liés à la SSI, ces modèles et théories apportent un éclairage appréciable sur le comportement des acteurs. L'introduction mettait l'accent sur l'importance particulière du rôle des décideurs pour une bonne prise en compte de la SSI

[1] Nous pouvons établir ici un parallèle avec la conduite d'une automobile et la souscription d'une assurance : « Les accidents, cela n'arrive qu'aux autres ». Le paiement de l'assurance est certain, mais va-t-on avoir un accident ? Sera-t-on remboursé correctement ?

[2] Au sens d'Agnew (1995).

		Nom de la théorie	Construit
Volet 1	TRA	Théorie de l'action raisonnée	Attitude vis-à-vis du comportement
			Normes subjectives
			Intention de comportement
	TPB	Théorie de prévision du comportement (*)	Maîtrise perçue du comportement
	MM	Modèle de la motivation	Motivation intrinsèque
			Motivation extrinsèque
Volet 2	TAM	Modèle d'acceptation de la technologie	Utilité perçue
			Facilité d'utilisation perçue
Volet 3	SLT	Théorie des liens sociaux	Attachement à l'entreprise
			Sens du devoir
			Implication dans son travail (temps consacré)
			Croyance dans les normes et l'autorité
	GDT	Théorie générale de la dissuasion	Dissuasion / Détection / Punition
Volet 4		Modèle des codes d'éthique	Effet des chartes d'utilisation et codes d'éthique
		Théorie des domaines de développement moral	Moralité des comportements

(*) Englobe la TRA

Tableau 1 : Vue synthétique des théories mobilisées et de leurs construits.

dans leur entreprise, il s'avère utile d'approfondir les spécificités liées à leur rôle.

1.2. Le comportement des décideurs

1.2.1. Une implication nécessaire de la part des décideurs

La littérature en SI insiste sur le fait que le directeur d'une entreprise doit non seulement être sensibilisé, mais aussi s'impliquer personnellement. A ce sujet, 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* » (p. 2).

Deux raisons expliquent pourquoi la direction devrait apporter son soutien lors de l'évolution d'un SI (Yap, 1989) : premièrement la direction, avec sa vision plus globale, se trouve dans une meilleure position que les analystes pour identifier les opportunités d'affaires dans l'exploitation des technologies de l'information. Ceci est plus particulièrement vrai dans une petite entreprise. Deuxièmement, la mise en place d'un SI génère de très importants investissements et se trouve souvent liée à des implications s'étendant à l'ensemble de l'entreprise.

Le directeur joue donc un rôle important, non seulement dans l'évolution d'un SI, mais aussi dans la mise en place d'une sécurisation des informations qui puisse être satisfaisante. Son implication est donc nécessaire : selon Longeon et Archimbaud, (1999), « *la détermination et la supervision de la politique de sécurité sont des fonctions de direction. Rien de valable ne peut se faire sans le directeur : encore faut-il qu'il en connaisse tous les enjeux. L'argument « la sécurité, c'est le problème d'un administrateur système » n'est-il pas une forme de démission ? N'est-ce pas avouer qu'on cherche des solutions techniques à des problèmes qui sont d'abord organisationnels ?* » (p. 19).

Pour Dutta et McCrohan (2002), comme il est impossible d'obtenir une sécurité parfaite, la direction doit réaliser les arbitrages appropriés coûts/bénéfices et décider de manière rationnelle du niveau de risque quelle souhaite assumer. Seule la direction est en position de réaliser ce choix. Friend et Pagliari (2000) confirment ceci : « *quelle que soit l'organisation, la direction est fondamentalement responsable de la sécurité. Toute action lancée ou problème résolu devrait être une résultante de l'intervention de la direction* » (p. 31).

Mais si cette implication et cette participation sont importantes, quels sont les facteurs qui vont faire qu'un décideur va être impliqué et va agir ?

1.2.2. Une compréhension de l'implication des décideurs

D'après Jarvenpaa et Ives (1991), l'implication psychologique du dirigeant est déterminée par la participation du dirigeant, son expérience, et l'environnement organisationnel de son entreprise.

Goodhue et Straub (1991), ont étudié la perception des risques en SI par les décideurs et ont montré que cette perception est anormalement basse, comparée à celle de l'ensemble des risques que court l'entreprise ; ils ne sont donc pas correctement préparés à faire face aux risques liés aux SI.

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

- l'environnement organisationnel (risque inhérent au secteur) ;
- l'étendue des efforts consentis pour contrôler ces risques ;
- facteurs spécifiques tels que la connaissance des sinistres précédents, l'expérience en SI.

L'intérêt de ce modèle réside dans le fait qu'il se destine spécifiquement à la SSI et permet de plus de déterminer un niveau d'implication du décideur dans la sécurité du SI de son entreprise.

Divers travaux ont confirmé que le soutien de la direction était essentiel pour l'allocation des ressources et l'obtention d'une adhésion des employés à la SSI (Avolio, 2000). En vertu de son rôle, la direction est capable d'agir comme un agent du changement afin de créer un environnement favorable (Lucas, 1981). Il a aussi été démontré que le dirigeant disposait de l'autorité

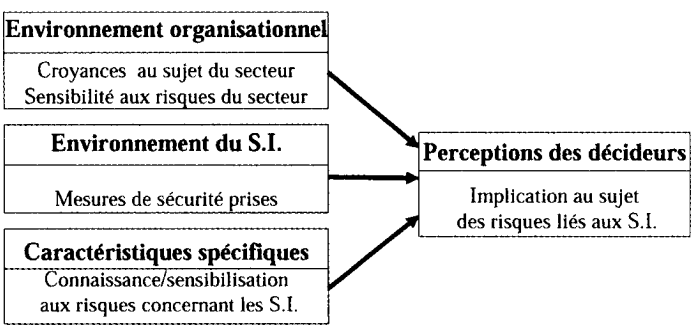

Figure 1 : Modèle de l'implication des décideurs, d'après Goodhue et Straub (1991).

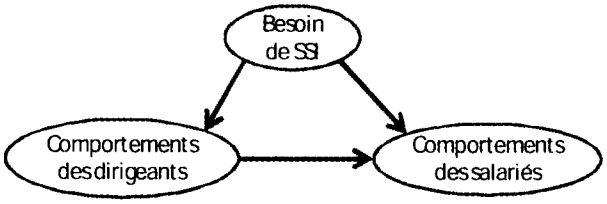

Figure 2 : L'incidence des comportements des dirigeants sur ceux des salariés.

nécessaire pour influencer les autres membres de l'entreprise, lui permettant ainsi de surmonter la résistance organisationnelle (Markus, 1983). Enfin, Grover (1993), a mis en évidence le fait que le soutien et l'implication de la direction transmettent des signaux forts dans toute l'organisation.

Ces derniers éléments font donc apparaître une troisième composante, l'incidence du comportement des dirigeants sur celui des salariés (figure 2), qui rend l'étude des dirigeants d'autant plus importante dans la recherche de facteurs d'amélioration de la SSI.

2. PROPOSITIONS, MÉTHODOLOGIE ET RÉSULTATS

2.1. Les propositions de recherche

L'étude de la littérature a permis de déterminer un cadre général d'analyse. Des théories et modèles ont été examinés, et nous avons discuté de la pertinence de les tirer de leur domaine d'origine pour les utiliser dans le cadre de la compréhension des comportements relatifs à la SSI. Afin de vérifier ceci, trois propositions de recherche vont être énoncées, concernant les dirigeants et les salariés.

Si les spécialistes de la sécurité et les scientifiques tels que Dutta et McCrohan (2002) ou Knapp *et al.* (2006) s'accordent sur le fait que le dirigeant ne doit pas déléguer la gestion de la sécurité, il n'a pas été possible d'identifier une étude ayant scientifiquement éprouvé l'incidence de cette délégation. La première proposition de recherche a pour objet de vérifier ceci :

Proposition 1 : Pour le dirigeant de PME, la gestion de la sécurité des SI ne peut pas être déléguée à un autre acteur.

La deuxième proposition concerne les salariés. On peut identifier dans le tableau 1 (cf. § 1.1) deux construits à dominante technique : la maîtrise perçue du comportement et la facilité d'utilisation perçue. Ces deux construits jouaient un rôle important dans l'acceptation et l'utilisation des TIC, mais ce rôle sera vraisemblablement à relativiser dans le cadre de comportements relatifs à la SSI.

D'autre part, l'analyse de la littérature a fait apparaitre que certains construits, comme l'utilité perçue, paraissaient peu pertinents pour cette étude.

Le but de la seconde proposition est donc non seulement de mettre en évi-

dence que les construits à dominante technique revêtent peu d'importance dans la compréhension des comportements des salariés relatifs à la SSI, mais aussi de faire ressortir dans les résultats les construits qui auront le plus d'incidence sur ces comportements, et donc d'identifier les facteurs de motivation des salariés dans ce domaine. Afin de vérifier ceci, on peut énoncer la proposition suivante :

Proposition 2 : Les comportements relatifs à la SSI des salariés en PME relèvent plus de caractéristiques personnelles que de compétences techniques.

Par caractéristiques personnelles, conformément à la revue de la littérature, il faut entendre des éléments liés aux salariés tels que la motivation, l'attachement à l'entreprise, le sens du devoir ou le sens moral. Cette deuxième proposition identifie les facteurs de motivation, mais quels sont les freins aux comportements relatifs à la SSI ? Comment atténuer ces freins et au contraire « faire levier » sur les facteurs de motivation pour motiver les salariés ? Ceci conduit à la proposition 3 :

Proposition 3 : Les comportements relatifs à la SSI des salariés en PME sont limités par des freins, une insuffisance en matière de comportements relatifs à la SSI peut être régulée par la mise en place de dispositifs de motivation.

Les deux parties suivantes présentent respectivement la méthodologie adoptée et les résultats obtenus.

2.2. La méthodologie

En référence à Yin (1989), une méthodologie qualitative et une approche interprétative du phénomène organisationnel observé ont été préférées pour de nombreuses raisons. Tout d'abord, dans leur grande majorité, les modèles examinés n'étaient pas destinés à l'étude des comportements relatifs à la SSI. Deuxièmement, même si certains modèles concernaient la SSI, les travaux qui ont servi à les bâtir ont été menés pour la plupart dans de grandes entreprises, appartenant souvent à une culture différente (surtout américaine), et basés parfois sur des publics trop spécifiques (des étudiants par exemple).

Troisièmement, Kotulic et Clark, (2004), dans leur article intitulé : « *pourquoi n'y a-t-il pas plus d'études scientifiques sur la sécurité des informations* », conseillent de pratiquer des entretiens en face à face. Ils suggèrent que dans un domaine aussi sensible que la sécurité, des études à grande échelle ne sont pas adaptées, car les entreprises craignent de divulguer des informations sensibles à un inconnu.

Enfin, 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). C'est bien une compréhension de comportements qui était souhaitée, de plus dans un domaine peu couvert par la théorie, ce qui justifiait non seulement une méthodologie qualitative mais aussi une démarche proche d'une étude de cas (Eisenhardt, 1996).

Nous avons donc opté pour une étude de cas allégée, qui consistait en plusieurs entretiens par entreprise : le dirigeant, la personne en charge du SI

ou de la SSI 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, lors de l'entretien le concernant, afin de s'assurer de leur disponibilité. Ces entretiens étaient accompagnés d'une visite complète de l'entreprise, en portant un intérêt particulier aux dispositifs informatiques, ce qui a permis d'établir l'estimation du niveau de sécurité évoquée dans la proposition 1.

La liste initiale des entreprises comportait 920 PME de 20 à 200 salariés, conformément à la typologie de PME établie par Julien et Marchesnay (1996), obtenues à partir du fichier des entreprises de la CCI de Montpellier. 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, ce qui pouvait biaiser les résultats. Un courrier a été envoyé aux 530 entreprises sélectionnées, leur proposant de participer à cette étude, 20 des courriers qui sont revenus en NPAI[3] n'ont pu être réexpédiés.

Neuf entreprises sur 510 ont répondu favorablement, soit un taux de réponses positives de 1,8 %. Sept entreprises ont décliné l'offre, évoquant toutes un manque de temps, ce qui explique en partie le faible taux de réponses. Un autre élément de réponse a été apporté par Kotulic et Clark (2004) qui ont souligné suite à leur étude que peu d'entreprises acceptent de parler de la SSI car elle constitue un sujet « envahissant » et « importun ». Eux-mêmes n'avaient d'ailleurs obtenu qu'un taux de réponse de 1,6 %.

30 entretiens ont été réalisés dans 9 entreprises différentes, ce qui a suffi à garantir un degré de certitude acceptable et une saturation théorique satisfaisante (Yin, 1989).

Ces entretiens étaient semi-directifs, pour cela un guide d'entretien a été constitué pour chaque type d'acteur. Sept thèmes principaux ont été abordés, divisés en sous-thèmes, ce qui correspondait à une vingtaine de questions. Les questions principales et les questions de relance ont été construites à partir des théories et modèles examinés dans la revue de la littérature, afin notamment de vérifier les facteurs de motivation et les freins aux comportements relatifs à la SSI des divers acteurs. Il était prévu dès le départ de croiser les discours (Wacheux, 1996), dans le but de vérifier le partage réel des rôles et qui était le véritable instigateur des actions mises en place.

Voici les principaux thèmes abordés :

- la vision de la sécurité ;
- la rôle déclaré par l'acteur ;
- la vision par l'acteur du rôle des autres acteurs ;
- les comportements des salariés ;
- les facteurs de motivation et freins ;
- les actions mises en place ou l'avis porté sur les actions mises en place ;
- les sinistres observés ou vécus.

[3] N'habite pas à l'adresse indiquée : entreprises n'existant plus ou ayant quitté la zone géographique sur laquelle portait l'étude.

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 et retranscrits donnant lieu à plusieurs centaines de pages à traiter. Des fiches d'entretiens comportant des éléments sur le contexte ont complété les informations enregistrées. Elles ont aussi servi à prendre en compte certaines informations mises en avant dans les modèles étudiés précédemment (sexe, âge, ancienneté, niveau d'éducation, niveau hiérarchique...). On pourra à ce sujet se référer aux tableaux 2 et 3 de l'annexe 2.

Une analyse lexicale réalisée à l'aide du logiciel Alceste a permis d'obtenir une première approche de la masse d'informations récoltées lors des entretiens, et de définir une typologie de dirigeants et de salariés ; ceci a servi à mieux aborder les analyses de discours « manuelles », intra et interentreprises menées par la suite.

Pour ces analyses de discours, trois matrices interentreprises (une par type d'acteur) et neuf matrices intra-entreprises (tous acteurs confondus, un extrait est visible en annexe 1) ont été réalisées, permettant de plus de croiser les discours entre eux. Vingt cinq tableaux d'analyse ont été ensuite établis, soit pour condenser les données au sens de Huberman et Miles (1991) afin de détailler un thème précis, soit pour croiser certaines informations : par exemple, pour déterminer le niveau d'implication d'un décideur, puis le relier au niveau d'action, etc.

De ces matrices et tableaux découlent les résultats présentés dans la partie suivante.

2.3. Les principaux résultats

En annexe 2, on peut trouver les caractéristiques des entreprises rencontrées (tableau 1), des dirigeants (tableau 2) et des salariés (tableau 3).

Le modèle présenté en figure 1 a permis d'évaluer l'implication du décideur dans la SSI de son entreprise. Un des éléments qui a permis d'estimer l'implication des dirigeants est présenté à titre d'exemple en annexe 3, tableau 1.

Proposition 1 : « Pour le dirigeant de PME, la gestion de la sécurité des SI ne peut pas être déléguée à un autre acteur ».

A un niveau opérationnel, quand le dirigeant est impliqué, il suit de près son service informatique ou gère lui-même les problèmes des salariés (Verbatim en Tableau 2, annexe 3). Il ne délègue donc pas la prise en charge de la SSI.

Seule l'entreprise 9 (E9 sur la figure 3) qui, avec 130 salariés était la PME de plus grande taille, disposait d'un service informatique, toutes les autres avaient recours aux services d'une société extérieure.

Sur la figure 3, les salariés des entreprises 4 et 6 (E4 et E6) font remonter les problèmes au dirigeant qui contacte la société extérieure. Dans l'entreprise 9, les salariés font remonter leurs problèmes au service informatique, malgré cela le dirigeant suit de près son activité et lui affecte des objectifs en termes de niveau de service. Dans l'entreprise 1, les salariés contactent directement la société extérieure.

Quand l'implication du dirigeant est faible, les principaux points qu'il

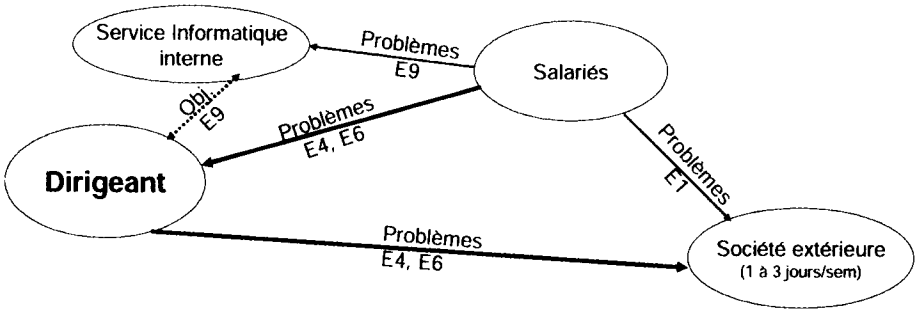

Figure 3 : Niveau opérationnel, dirigeant impliqué.

évoque pour se justifier sont le manque de temps, d'argent et de connaissances en SI. Dans ce cas, le dirigeant délègue la prise en charge de la SSI, mais nous avons vu qu'il n'y avait aucun responsable du SI et *a fortiori* aucun responsable de la sécurité du SI (RSI).

Le phénomène suivant est apparu : **c'est un salarié qui assume de manière informelle** le rôle de RSI et va gérer les problèmes des salariés. Sur le schéma suivant, les entreprises 2, 5 et 8 font remonter leurs problèmes à ce « salarié-RSI » (cf. figure 4).

Cette prise en charge informelle apparait aussi lors des décisions plus globales en matière de SSI.

A un niveau stratégique, quand le dirigeant est impliqué, il gère la SSI et son évolution, soit en liaison avec le service informatique interne (E9), soit avec la société extérieure (cf. figure 5).

Quand il n'est pas impliqué, c'est encore le « salarié-RSI » qui gère cette évolution de la sécurité, mais sous le contrôle du dirigeant. Ce salarié doit alors négocier avec le dirigeant certaines décisions, et le dirigeant peut donc s'avérer constituer un frein dans certains cas : le salarié-RSI n'est pas forcément crédible pour le patron, car il n'a pas de diplôme dans le domaine, et encore moins de fonction « officielle » (cf. figure 6).

Les fonctions des trois salariés « RSI » étaient très diverses : un chargé de mission (E2), un responsable qualité (E5) et un dessinateur (E8). Comme cette

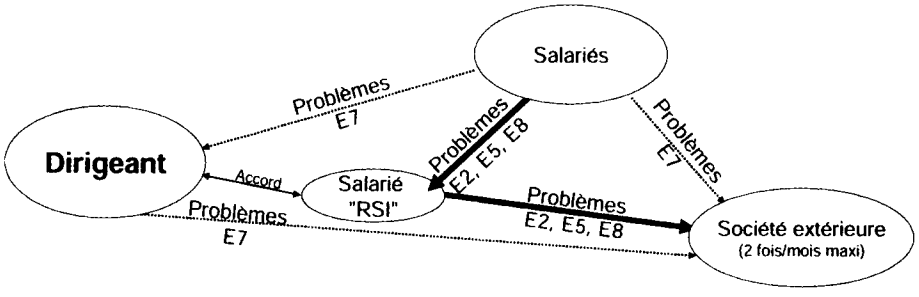

Figure 4 : Niveau opérationnel, dirigeant NON impliqué.

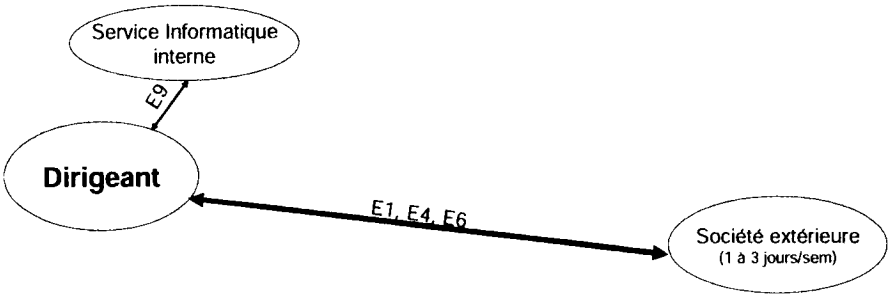

Figure 5 : Niveau stratégique, dirigeant impliqué.

prise en charge informelle n'avait pas été anticipée et que trois cas seulement ont été identifiés, il est difficile de donner un profil-type, par contre il est possible d'avancer certaines constantes qui pourraient constituer les bases d'une étude ultérieure :

- aucun n'avait de compétences préalables dans le domaine de la sécurité ou des technologies de l'information et tous se sont donc « formés sur le tas » ;
- tous ont fait des études supérieures ;
- tous sont des hommes.

Toujours dans le cadre de cette proposition 1, il s'agissait de déterminer aussi l'effet de cette délégation. Il s'est avéré nécessaire de créer un instrument simplifié de mesure du niveau de sécurité de chaque PME, comportant 17 points d'appréciation du niveau de sécurité, relatifs aux systèmes techniques et aux pratiques liées à la SSI.

Dans le cas où le dirigeant était impliqué dans la SSI, le niveau de sécurité était en général bon voire très bon. Les salariés percevaient aussi cette implication du dirigeant et se sentaient eux-mêmes plus impliqués dans la SSI que les salariés des entreprises dans lesquelles le dirigeant n'était pas impliqué.

Quand le dirigeant était peu impliqué, dans la moitié des cas le niveau de sécurité était très insuffisant, dans l'autre moitié des cas le niveau restait assez satisfaisant, avec pour explication les aspects financiers et l'aptitude du salarié-RSI à convaincre le dirigeant d'investir.

Ces résultats constituent à notre connaissance la première confirmation sur le terrain de ce que déclarent de nombreux scientifiques sur l'importance du rôle du dirigeant (Yap, 1989 ; Avolio, 2000), et sur l'effet négatif de la délégation (Longeon et Archimbaud,

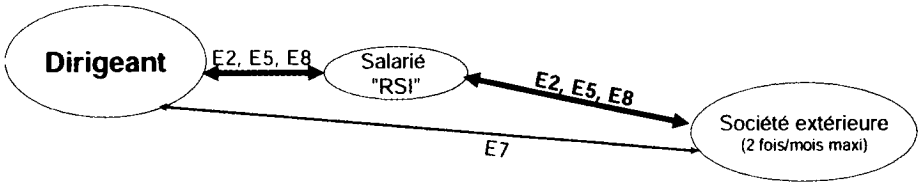

Figure 6 : Niveau stratégique, dirigeant NON impliqué.

1999 ; Friend et Pagliari, 2000). Cet effet négatif doit pourtant être nuancé, du fait de l'apparition de ce salarié-RSI qui contrebalance dans une certaine mesure la baisse du niveau de sécurité.

Proposition numéro 2 : « *Les comportements relatifs à la SSI des salariés en PME relèvent plus de caractéristiques personnelles que de compétences techniques* ».

Dans le tableau 3 de l'annexe 3, on peut trouver quelques extraits du verbatim des salariés.

Les principaux facteurs de motivation identifiés sont :

- les motivations ou convictions personnelles ;
- la préservation de l'intimité ;
- les motivations liées au poste ;
- les motivations liées à l'entreprise ;
- l'habitude ;
- le vécu.

Ces facteurs sont bien liés à des caractéristiques personnelles. Au sujet des compétences techniques, l'analyse lexicale a mis en évidence des préoccupations différentes lors des entretiens. S'il s'est avéré que les quatre salariés utilisant/maîtrisant plus particulièrement les SI faisaient état de comportement relatifs à la sécurité plus techniques (sauvegardes, antivirus, protection des données du disque dur), les douze autres salariés parlaient de protection des informations au sens large, incluant la confidentialité des propos, fermeture des bureaux et armoires, ne pas laisser trainer de papiers à portée de vue, broyer/détruire les documents jetés. Si l'on prend donc en compte les comportements globaux relatifs à la sécurité des SI, techniques et non-techniques, le niveau d'utilisation des SI ne joue pas un rôle notable en comparaison avec les caractéristiques personnelles identifiées.

Cette étude a aussi pris en compte les facteurs explicatifs traditionnels[4] des comportements des acteurs face aux SI tels que l'âge, le niveau de formation, le niveau hiérarchique ou encore le sexe (cf. annexe 2, tableau 3). Les résultats de l'analyse lexicale et de l'étude des facteurs de motivation avancés lors des entretiens confirment la propension des hommes à avoir des comportements plus « techniques » que les femmes en matière de sécurité des SI. Sur le plan des comportements relatifs à la sécurité des SI, qu'ils soient donc techniques ou non, certaines tendances ressortent[5], notamment au niveau des motivations annoncées pour ces comportements par les 16 salariés :

- les cadres évoquent la « préservation de l'intimité » (5 cadres sur 10, contre 0 non-cadre sur 6) ;
- les femmes évoquent plus leur poste ou leur fonction comme élément de motivation que les hommes (4 femmes sur 9, contre un homme sur 7) ;
- l'âge joue sur l'évocation de « la loyauté à l'entreprise » (4 salariés de

[4] En raison d'un manque de place, ces éléments ne figurent pas dans la revue de la littérature. On pourra se référer par exemple aux travaux de Venkatesh *et al.* (2003) ou encore à ceux de Wixom et Todd (2005).
[5] La taille de l'échantillon ne permet pas de prétendre généraliser ces résultats, qui sont plutôt à considérer comme des pistes de recherches.

		Nom de la théorie	Construit	Adéquation avec les observations (**)
Volet 1	TRA	Théorie de l'action raisonnée	Attitude vis-à-vis du comportement	x
			Normes subjectives	xx (pour l'influence de la hiérarchie)
			Intention de comportement	xx
	TPB	Théorie de prévision du comportement (*)	Maîtrise perçue du comportement	
	MM	Modèle de la motivation	Motivation intrinsèque	xxx
			Motivation extrinsèque	
Volet 2	TAM	Modèle d'acceptation de la technologie	Utilité perçue	
			Facilité d'utilisation perçue	
Volet 3	SLT	Théorie des liens sociaux	Attachement à l'entreprise	xxx
			Sens du devoir	xxx
			Implication dans son travail (temps consacré)	
			Croyance dans les normes et l'autorité	x
	GDT	Théorie générale de la dissuasion	Dissuasion / Détection / Punition	
Volet 4		Modèle des codes d'éthique	Effet des chartes d'utilisation et codes d'éthique	Aucune entreprise n'en avait
		Théorie des domaines de développement moral	Moralité des comportements	x

(*) Englobe la TRA
(**) Le nombre correspond à x faible, xx moyen, xxx fort

Tableau 2 : Adéquation des résultats de l'étude avec les construits.

plus de 43 ans sur 10, contre 1 sur les 6 d'âge inférieur) ;

- inversement les plus jeunes évoquent le fait que les comportements sont « habituels », « un reflexe » ou « naturels » (4 entre 25 et 33 ans contre 1 seul de 53 ans).

Le tableau ci-dessus réalise un bilan de l'ensemble des résultats[6] de l'étude. On observe que trois théories correspondent au moins partiellement : la TRA, deux des quatre construits de la théorie des liens sociaux (SLT), et la motivation intrinsèque. Par contre il n'a été identifié aucune trace d'une motivation extrinsèque, de l'utilité perçue d'un comportement en SSI ou d'une motivation liée à la facilité d'utilisation. Une mention spéciale est à accorder à la théorie de la dissuasion qui n'a pas du tout été confirmée, malgré le fait que c'était la seule spécifique à la SSI, personne ne s'étant déclaré sensible à une quelconque menace ou n'ayant été sanctionné suite à un incident de sécurité.

Enfin, on notera l'importance de l'habitude et du vécu dans les comportements liés à la SSI, ce qui n'est quasiment pas pris en compte dans les théories et modèles étudiés : ces deux élément se retrouvent, de manière très partielle, dans le construit «attitude vis-à-vis du comportement».

Proposition numéro 3 : « *Les comportements relatifs à la SSI des salariés en PME sont limités par des freins, une insuffisance en matière de comportements relatifs à la SSI peut être régulée par la mise en place de dispositifs de motivation* ».

Les freins correspondaient premièrement la balance entre le temps passé à travailler et le temps consacré à la sécurité : « *un quart d'heure passé à faire mes sauvegardes, c'est un quart d'heure de perdu dans mon travail* ».

Deuxièmement un manque d'information, sensibilisation, formation. On rencontre des affirmations du type : « *ce n'est pas mon problème* », « *il n'y a pas de risque* ».

Enfin la complexité et le manque de support ont aussi été évoqués comme des freins.

[6] Nous rappellerons que seuls les principaux éléments ont été commentés.

Si l'on se reporte au tableau 2, on relève qu'il y a plutôt une IN-utilité perçue des comportements liés à la SSI, et que les éléments techniques, s'ils ne constituent pas des facteurs de motivation, peuvent au contraire limiter les comportements relatifs à la SSI (non-facilité, non-maîtrise).

Les dispositifs de motivation identifiés sont, par ordre de faisabilité décroissant :

- l'influence de la hiérarchie ;
- l'automatisation des actions liées à la sécurité (sauvegardes, mise à jour...) ;
- l'utilisation de guides et chartes ;
- l'amélioration du support et de l'aide aux utilisateurs ;
- des campagnes de sensibilisation et de formation.

Si l'on examine plus en détails certains de ces points, l'influence de la hiérarchie représente l'un des facteurs à la fois le plus important et le plus facile à mettre en œuvre si l'on tient compte des contraintes de temps ou d'argent : le dirigeant devrait donc faire passer un message à ses salariés d'une manière ou d'une autre. L'automatisation permettrait de limiter les contraintes portant sur les salariés, par contre la sensibilisation et la formation, qui sont considérées comme très efficaces, sont aussi les moyens les plus coûteux en temps et en argent.

Toujours en se référant au tableau 2, on remarque qu'il est donc possible de mobiliser certains construits, dans le cadre des mécanismes de limitation de ces lacunes, en matière de comportements positifs pour la SSI de l'entreprise. Le modèle des codes d'éthique peut aussi être mobilisé dans le cadre de la mise en place de chartes de sécurité.

Enfin, la proposition 3 fait ressortir des éléments qui pourraient être intégrés dans des campagnes de sensibilisation et de formation, qui devraient donc majoritairement intégrer des éléments non-techniques tels que ceux valorisant l'attachement à l'entreprise, la responsabilité liée au poste, etc.

Ce bilan résume les principaux résultats relatifs aux trois propositions énoncées :

- P1 : Elle est partiellement confirmée. Même s'il est effectivement souhaitable que le dirigeant gère lui-même la sécurité de son entreprise, il a été toutefois mis en évidence qu'une délégation sans conséquences néfastes reste possible. Il a été principalement mis en évidence un phénomène de délégation informelle qui n'avait pas été décelé dans les travaux scientifiques ;
- P2 : Elle est confirmée. Elle fait apparaître l'importance majeure des caractéristiques personnelles, en contradiction avec certains construits des modèles consacrés à l'appropriation et à l'adoption des TIC tels que l'utilité perçue ;
- P3 : Elle est confirmée. Cette proposition a permis d'identifier les freins et possibilités d'action concernant les comportements en SSI.

CONCLUSION

Cette recherche sur les comportements relatifs à la sécurité au sein des organisations avait pour but principal

d'apporter un éclairage sur des comportements organisationnels, dans un domaine sensible, qui étaient peu balisés en sciences de gestion. Elle comprend les limites inhérentes à la méthodologie qualitative adoptée pour étudier ce sujet. Ce travail est aussi limité par le dispositif d'enquête auprès de 9 PME, il gagnerait à être éprouvé par d'autres méthodologies auprès d'autres organisations. Il serait aussi souhaitable, lors de prochaines études, de mieux prendre en compte le secteur d'activité. Il s'agirait alors d'identifier par exemple les organisations qui sont les plus sensibles à la confidentialité des données telles que des entreprises appartenant à des secteurs innovants ou de pointe, ou encore celles dépendant plus particulièrement de la disponibilité et l'intégrité de leurs informations (activité de vente à distance basée uniquement sur l'utilisation d'un fichier client par exemple).

Une étude à grande échelle par questionnaire pourrait être tentée, mais elle se verra confrontée au problème aussi rencontré par Kotulic et Clark, (2004) : les entreprises ne souhaitent pas traiter de la SSI à distance, avec des personnes inconnues. Il faudrait donc s'adresser à plusieurs milliers d'entreprises pour disposer d'un nombre de réponses satisfaisant.

Cet article apporte toutefois une contribution aux théories sur les comportements relatifs à la SSI, non seulement au sujet des salariés, mais aussi des dirigeants.

Concernant les dirigeants, les résultats obtenus étaient en phase avec les éléments ressortant de l'étude de la littérature : la mauvaise perception des risques encourus, la difficulté de l'évaluation de la valeur des informations sous forme électronique, l'importance du rôle du dirigeant dans la prise en compte des problématiques liées à la SSI et l'influence du dirigeant sur les comportements des salariés.

Au sujet des salariés, nous avons pu constater que les comportements en SSI allaient au-delà de la technique et de l'appropriation des technologies, ce qui conduit à privilégier certaines théories comportementalistes telles que le modèle de la motivation intrinsèque et la théorie de prévision du comportement (TPB) et certaines théories tirées de la psychologie (théorie des liens sociaux) au détriment de théories liées à l'adoption des technologies par exemple.

Sur un plan managérial, ces travaux peuvent servir à mettre en place une sensibilisation et une mise en garde des dirigeants au sujet de la délégation, qui peut s'avérer risquée et doit donc être réalisée en prenant des précautions. De la même manière, l'influence bénéfique des dirigeants sur les comportements des salariés a été confirmée, cette influence doit donc être mise en avant et développée.

Concernant les salariés, des facteurs motivationnels qui sortent largement du cadre des problèmes techniques ont été mis en évidence, ce qui avait été peu développé jusqu'à présent. Cet éclairage sur les comportements rend possibles certaines interventions, comme la mise en place d'une sensibilisation plus ciblée qui prenne en compte les principaux facteurs de motivation et les freins aux comportements qui ont été identifiés.

De même, les caractéristiques personnelles étant importantes dans les com-

portements relatifs à la SSI (proposition 2), il serait souhaitable de les prendre en compte lors du recrutement de salariés.

Ce domaine de la SSI mérite des études plus approfondies, voici quelques pistes que nous proposons :

Il a été constaté que si l'implication des dirigeants avait effectivement une grande influence sur les comportements des salariés, d'autres facteurs d'explication de leurs comportements pourraient être explorés, tels que par exemple la piste de la « propension à agir ».

Le cas de la délégation n'étant pas obligatoirement synonyme d'un niveau de sécurité insuffisant, il serait intéressant de déterminer quels seraient les facteurs d'une délégation dont les effets négatifs seraient minimisés.

Il a été confirmé que l'implication des dirigeants se traduisait dans les comportements des salariés. Une étude plus approfondie permettrait de mieux comprendre comment se fait cette transmission de l'implication. Certaines théories ou domaines scientifiques pourraient être mobilisés, comme par exemple les théories relatives aux comportements de mimétique ou l'influence sociale.

Tout comme des modèles concernant les comportements d'acceptation et d'utilisation des technologies existent, une modélisation des comportements des salariés relatifs à la SSI pourrait être mise en place.

Toutefois l'apport principal de cette étude réside dans le phénomène de prise en charge informelle de la SSI par un salarié. Trois principales problématiques en découlent :

Le premier point concerne « l'apparition » de cette prise en charge. Elle peut se faire lors d'un recrutement spécifique : il s'agira alors de rechercher les potentiels les plus susceptibles d'assumer cette charge. Afin de faciliter ce recrutement de potentiels, des études pourraient être menées pour déterminer s'il existe un profil-type de « salarié-RSI » et si c'était le cas, d'en identifier les principales caractéristiques.

Il est aussi possible de favoriser l'« apparition » de cette prise en charge par un salarié existant. Des théories telles que la théorie de l'aversion au risque, la théorie de l'agence ou la théorie de l'incitation pourraient ainsi être mobilisées. Le troisième point correspond à l'étude des moyens de faciliter la tâche d'un salarié-RSI, vu le manque d'influence et de crédibilité identifiés. Des recherches seraient donc bienvenues dans ce domaine.

BIBLIOGRAPHIE

Adams, A., Sasse, M.A. (1999), « Users are not the enemy », *Communications of the ACM*, Vol. 42, n° 12, p. 40-46.

Agnew, R. (1995), « Testing the leading crime theories: an alternative strategy focusing on motivational process », *Journal of research in crime and delinquency*, Vol. 32, n° 4, p. 363-398.

Ajzen, I. (1991), « The Theory of Planned Behavior », *Organizational Behavior and Human Decision Processes*, Vol. 50, n° 2, p. 179-211.

Ajzen, I., Fishbein, M. (1980), *Understanding attitudes and predicting social behaviour*, Prentice Hall, Englewood cliffs, NJ, 278 p.

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.

CERT (2007), *CERT/CC: Statistics 1988-2006*, Computer Emergency Response Team, www.cert.org.

CLUSIF (2004), *Politiques de sécurité des systèmes d'information et sinistralité en France*, 42 p.

Davenport, T. (2002), Privilégier l'information sur la technologie, accédé en novembre 2008 sur le site : http://www.lesechos.fr/formations/manag_info/articles/article_1_1.htm

Davis, F.D. (1989), « Perceived usefulness, perceived ease of use, and user acceptance of information technology », *MIS Quarterly*, Vol. 13, n° 3, p. 319-339.

Davis, F. D., Bagozzi, R. P., Warshaw, P. R. (1989), « User Acceptance of Computer Technology: A Comparison of Two Theoretical Models », *Management Science*, Vol. 35, n° 8, p. 982-1002.

Davis, F. D., Bagozzi, R. P., Warshaw, P. R. (1992), « Extrinsic and Intrinsic Motivation to Use Computers in the Workplace », *Journal of Applied Social Psychology*, Vol. 22, n° 14, p. 1111-1132.

Deci, E.L., Ryan, R.M. (1985), *Intrinsic motivation and self-determination in human behavior*, Plenum Press, NY, 371 p.

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

Dutta, A., 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.

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

Gattiker, U.E., Kelley, H. (1999), « Morality and computers: Attitudes and differences in moral judgments », *Information Systems Research*, Vol. 10, n° 3, p. 233-254.

Goodhue, D.L., Straub, D.W. (1991), « Security concerns of systems users: a study of perceptions of the adequacy of security measures », *Information and Management*, Vol. 20, n° 1, p. 13-27.

Gottfredson, M.R., Hirschi, T.A. (1990), *A General Theory of crime*, Stanford University Press, CA, 297 p.

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., 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.

Harrington, S.J. (1996), « The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions », *MIS Quarterly*, Vol. 20, n° 3, p. 257-278.

Huberman, A.M., Miles, M. B. (1991), *Analyse des données quantitatives : Recueil de nouvelles méthodes*, De Boeck, Bruxelles, 480 p.

INSEE (2006), *Tableaux de l'Économie Française*, INSEE Références, Paris, 204 p.

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

Jenkins, P.H. (1997), « School delinquency and the school social bond », *Journal of research in crime and delinquency*, Vol. 34, n° 3, p. 337-367.

Julien, P.A., Marchesnay, M. (1996), *L'entrepreneuriat*, Economica, Paris, 112 p.

Knapp, K.J., Marshall, T.E., Kelly Rainer, R., 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.

Kotulic, A., Clark, J.G. (2004), « Why there aren't more information security research studies », *Information and Management*, Vol. 41, n° 5, p. 597-607.

Longeon, R., Archimbaud, J.L. (1999), *Guide de la sécurité des SI à l'usage des directeurs*, CNRS, Paris.

Lucas, H.C. Jr (1981), *Implementation: the key to successful information systems*, Columbia University Press, NY, 208 p.

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

Mitchell, R.C., Marcella, R., Baxter, G. (1999), « Corporate information security management », *New Library World*, Vol. 100, n° 1150, p. 213-227.

Monnoyer, M.C. (2003), *Le dirigeant confronté à la 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, 275 p.

Reix, R. (2004), *Systèmes d'information et management des organisations*, Vuibert, Paris, 486 p.

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

Straub, D.W., Welke, R. (1998) « Coping with systems risk: security planning models for management decision making », *MIS Quarterly*, Vol. 22, n° 4, p. 441-469.

Taylor, S., and Todd, P. A. (1995), « Assessing IT Usage: The Role of Prior Experience », *MIS Quarterly*, Vol. 19, n° 2, p. 561-570.

Vallerand, R. J. (1997), « Toward a Hierarchical Model of Intrinsic and Extrinsic Motivation », in *Advances in Experimental Social Psychology*, Vol. 29, M. Zanna (ed.), Academic Press, New York, p. 271-360.

Venkatesh, V., Speier, C. (1999), « Computer Technology Training in the Workplace: A Longitudinal Investigation of the Effect of the Mood », *Organizational Behavior and Human Decision Processes*, Vol. 79, n° 1, p. 1-28.

Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D. (2003), « User acceptance of information technology: Toward a unified view », *MIS Quarterly*, Vol. 27, n° 3, p. 425-478.

Wacheux, F. (1996), *Méthodes qualitatives et recherche en gestion*, Economica, Paris, 290 p.

Wixom, B. H., Todd, P. A. (2005), « A Theoretical Integration of User Satisfaction and Technology Acceptance », *Information Systems Research*, Vol. 16, n° 1, p. 85-102.

Yap, C.S. (1989), « Issues in managing information technology », *Journal of operational research society*, Vol. 40, n° 7, p. 649-658.

Yin, R.K. (1989), *Case study research: design and methods*, Sage Publications, Londres, 168 p.

ANNEXE 1 : MATRICE INTRA-CAS DE L'ENTREPRISE 6 (EXTRAIT : THÈMES ET ACTEURS LIMITÉS)

Type d'acteur / Thème	Dirigeante	Salarié 1	Salariée 2
Vision de la sécurité des informations	*"On est sensibilisés par rapport au secret médical et au secret professionnel de manière générale"* *"On est sensibilisés aussi par rapport aux échanges que l'on peut avoir avec l'extérieur"* (peur d'une mauvaise publicité) *"On n'aurait pas de perte totale d'information, dans la mesure où on a toujours un dossier papier"*	*"un système hermétique (...) ça c'est fondamental"* *"Que n'importe qui ne puisse pas pénétrer n'importe comment dans les fichiers, dans les dossiers des patients, dans les dossiers de la comptabilité"* *"ce serait quand même d'avoir cette quasi certitude que qui doit et peut voir l'information la voit, et qui ne doit pas la voir ne la voit pas"*	*"Que les informations n'échappent pas au public" Que le cas reste confidentiel* Si tout est bloqué, ils peuvent quand même fonctionner par téléphone et papier. Ce ne serait pas moins pratique ni plus compliqué mais moins officiel.
Rôle déclaré par l'acteur	*"c'est moi qui suis responsable" de la "sécurité au sens large", mais "sur un plan plus informatique on n'a personne de spécifique".* *"Peut-être que ça m'est personnel, j'y suis sensible, mais je crois que cela fait partie de la culture maison où on discute assez librement des patients"*	[redacted]	
Qui prend en charge la sécurité et rôle joué	Elle, et quand il y a un problème *"j'appelle en fait notre prestataire informatique"* Cela peut aussi remonter à sa collaboratrice (resp. compta). Le prestataire vient tous les 15 jours.	Le prestataire extérieur. La directrice et l'attachée de direction "sont quand même un peu les pivots". La direction apporte un soutien.	La directrice, l'assistante de direction (# resp. comptable)
Comportement des employés	*"Comme on a quand même pas mal de personnes, je pense en particulier au domaine médical, les gens ne font pas forcément"* *"Certains s'y connaissent en informatique, mais d'autres, le style de ce qui est ici, des fois ce sont des demandes ... bon. Faut pas faire deplacer le prestataire pour ça."* Les infirmières : *Elles sont soucieuses de ce qui est sécurité de l'information, je mettrais l'informatique à part (...) vous n'allez jamais pouvoir accéder à leur bureau où des dossiers traineraient. Sur l'informatique, (...) je pense qu'elles ne s'y connaissent pas suffisamment, elles ont des fois du mal à utiliser l'outil*	*"Fermer l'ordinateur en partant et fermer la porte en partant."* Ne fait pas de sauvegardes, non concerné. *"on a un informaticien qui s'occupe de ça"* Ne change pas son mot de passe, il fait 5 caractères.	*"Quelque part s'il y a un virus ou pas, ça nous concerne pas directement, en fait il y a l'informaticien qui est là pour ça"* *"Broyer les papiers, je pense que ce sont souvent les mêmes qui le font en fin de compte. Mais on y a été pas mal sensibilisés par l'accréditation tous ces trucs là"* Leur salle est fermée à clé (pharmacie + dossiers + ordinateur) : seuls médecins et infirmières ont la clé (ni dames service, ni stagiaires). Rappelle à l'ordre les imprudents
Facteurs de (dé)motivation	[redacted]	*" il n'y a pas vraiment de règlement interne, il y a une prise de conscience collective qui s'est beaucoup passée autour du processus, justement, de l'accréditation (...) [une conscience] de la preservation du secret.* *"c'est bien intégré, c'est pas une obligation. C'est volontaire, mais enfin un petit peu machinal, quoi. Ça se fait naturellement je dirais"*	Des habitudes à prendre. Ce n'est pas une obligation : *"je fais partie de la génération un peu des infirmiers où on a été pas mal pris dans ça au niveau de l'école"* La sécurité doit être réalisée par l'informaticien (prestataire extérieur). Pense que eux ne peuvent pas perdre d'infos (sauvegardes)

ANNEXE 2 : CARACTÉRISTIQUES DES ENTREPRISES ET DES ACTEURS INTERROGÉS

Entreprise	Date de création	Nombre de salariés		Activité
		Permanents	Temporaires	
1	21/12/2001	15	20	Commercialisation de produits diététiques et biologiques
2	01/07/2001	6	46 (*)	Pépinière d'entreprises. (*) Les entrepreneurs sont comptés comme salariés temporaires.
3	28/07/1993	21	0	Entreprise de forages
4	01/07/1990	20	0	Conception, fabrication et vente de produits plastiques
5	01/08/1988	19	0	Fabrication et commercialisation de peintures
6	01/11/1972	70	0	Institut psychiatrique
7	01/01/1978	46	0	Exploitation de carrières, fabrication et commercialisation de produits liés au bâtiment
8	01/04/1990	30	10	Travaux de charpentes et couvertures
9	29/09/2000	130	0	Conception, réalisation et vente de systèmes photovoltaïques et thermiques

Tableau 1 : Les entreprises rencontrées.

Entreprise	Date de création	Nombre de salariés		Activité
		Permanents	Temporaires	
1	21/12/2001	15	20	Commercialisation de produits diététiques et biologiques
2	01/07/2001	6	46 (*)	Pépinière d'entreprises. (*) Les entrepreneurs sont comptés comme salariés temporaires.
3	28/07/1993	21	0	Entreprise de forages
4	01/07/1990	20	0	Conception, fabrication et vente de produits plastiques
5	01/08/1988	19	0	Fabrication et commercialisation de peintures
6	01/11/1972	70	0	Institut psychiatrique
7	01/01/1978	46	0	Exploitation de carrières, fabrication et commercialisation de produits liés au bâtiment
8	01/04/1990	30	10	Travaux de charpentes et couvertures
9	29/09/2000	130	0	Conception, réalisation et vente de systèmes photovoltaïques et thermiques

NB : La colonne « responsabilités réelles » a été rajoutée pour identifier les dirigeants qui prenaient en charge la sécurité du SI de leur entreprise lorsqu'il n'y avait aucun service informatique. De même, dans l'entreprise 7, la responsable administrative remplace souvent le directeur qui est peu présent dans l'entreprise, elle influence beaucoup le directeur.

Tableau 2 : Caractéristiques des dirigeants.

Entreprise	Initiales	Sexe	Age	Fonction	Statut	Expérience	
						Fonction	Ancienneté
1	NC	F	32	Resp. Service client/qualité client	Cadre	1	3
1	PH	M	43	Dirigeant cellule appel	Cadre	6	6
2	LP	F	41	Resp. Comptabilité	Cadre	15	4,5
2	Impossible						
3	Impossible						
4	IC	F	68	Co-Directrice (créatrice)	Cadre	50	16
4	SL	F	33	Standard / Accueil	NC	5	1
5	MV	M	59	Directeur technique	Cadre	38	35
5	CI	F	58	Resp. Comptabilité	Cadre	38	22
6	MA	M	53	Psychiatre - Actionnaire	Cadre	23	15
6	MC	F	27	Infirmière	NC	5	5
6	MJB	F	55	Secrétaire Comptable	NC	16	16
7	JT	M	50	Adjoint resp. assurance qualité	NC	2,5	2,5
7	PO	F	43	Comptable	NC	20	1
8	VH	M	25	Dessinateur/Exécution	NC	2,5	2,5
8	P	M	43	Responsable Atelier	Cadre	1	8
9	MC	M	28	Ingénieur R&D	Cadre	3	3
9	SV	F	30	Resp. RH et juridique	Cadre	5	5

Tableau 3 : Caractéristiques des salariés.

ANNEXE 3 : UNE SÉLECTION DE VERBATIM

Nous avons sélectionné quelques verbatim à titre d'exemple ou les plus significatifs parmi les tableaux dont nous disposons.

Entreprise 1 : J.J.H	Entreprise 2 : N.L.	Entreprise 4: M.G	Entreprise 5 : J.F.C.
"Je considère que cela crée de la valeur d'avoir des procédures". *"Je dirais, c'est pas très rentable, mais d'un autre côté, à terme, c'est indispensable".*	*"Je n'ai pas peur".* *"je peux concevoir qu'on sécurise des informations mais (...), moi je ne sécurise rien et j'ai rien à cacher, quoi."* *"Au pire mon entreprise disparaît et en fait est-ce que c'est très important ?".* La comptabilité est sécurisée : pour le fisc et pour "*respecter le travail du comptable*".	*"La sécurité de l'information est indispensable, parce que (...) ce que l'on fait ou voit dans l'entreprise doit rester dans l'entreprise."* *"Il faut une certaine paranoïa, une paranoïa raisonnée".*	*"Il est évident qu'il faut préserver nos formules, (...) mais c'est pas absolument essentiel."* *"Qu'on n'ait plus accès à nos sauvegardes et que le système informatique soit en panne, là on serait vraiment dans la mouise".* *"Le risque ne me paraît pas énorme dans la mesure où on n'est pas dans des technologies de pointe".* *"Si l'informatique tombe en panne et qu'on ne peut plus enregistrer les commandes avec l'ordinateur, on le fera à la main."*

Tableau 1 : Représentation de la sécurité pour les dirigeants d'entreprises.

Entreprise 1 : JJH	Entreprise 4 : M.G.	Entreprise 6 : V.A.	Entreprise 9 : S.G.
Pour l'informatique : "On" a refait. "*j'ai fait faire*". **Segmentation des infos** Arrêt de la location de fichiers **A mis en place toutes les procédures sécuritaires existantes.** "*Les vendeurs, le meilleur moyen de les protéger contre eux-mêmes, c'est de leur parler des produits qu'ils ont à vendre*". Ordinateurs des intérimaires bridés : pas de cédérom Droits d'accès protégés par mot de passe. Modernisation sauvegardes **Achat armoires "fortes"** "*C'est une impulsion mais cela reste "artisanal".*	**Elle nous dit s'occuper de tout (gère la société extérieure).** "*Je m'occupe avec ma collaboratrice des sauvegardes quotidiennes*" *"La perte d'activité et de C.A. sont chiffrés et assurés".* Limite les visites. S'assure que les visiteurs sont surveillés. Binôme prévu (si maladie) Documents sortants en PDF (pb onglets Excel). "*Quand je vois une déviation légère, même légère, alors là je remets la sauce totale. Des fois qu'ils aient oublié autre chose aussi ...*"	***"c'est moi qui suis responsable" de la "sécurité au sens large"****, mais "sur un plan plus informatique on n'a personne de spécifique".* Les problèmes informatiques lui remontent directement. *"Peut-être que ça m'est personnel, j'y suis sensible, mais je crois que cela fait partie de la culture maison où on discute assez librement des patients"* *"Les normes de sécurité évoluent beaucoup et du coup cela nous laisse peu de marge de manœuvre budgétaire". "On suit plus les textes qu'autre chose".* Informatisation des prescriptions. Renouvèlement du parc (plus de lecteur de CD) Interdiction de charger des logiciels.	**Elle gère le responsable informatique.** *"C'est plutôt un rappel à l'ordre en permanent. Quand les gens ne le font pas, au moins ils se disent, «elle agit comme ça »".* *"Il y a tellement de cas de figure différents (...) qu'on n'a jamais chiffré [les sinistres]"* **A inclus la sécurité dans le contrat du RSI et du responsable sécurité.** Mes informations, "*j'y fais très attention*", mais "*je suis pas derrière chaque poste de travail*" Avant l'automatisation ne mettait jamais à jour son antivirus.

Tableau 2 : Actions menées par les dirigeants impliqués.

Salarié 52	Salariée 63	Salarié 71	Salarié 81
"Les gens n'ont pas à savoir ce qui se fait ici, et ce qu'il est..." *"Dans notre domaine bien précis, c'est surtout la formulation de toutes les peintures qui doit être confidentielle. Les prix d'achat également. 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"*	Ses comportements sont tous volontaires. *"C'est une question de responsabilité, de conscience professionnelle si vous préférez !"* *"C'est lié à la fonction".* *"Ça me paraît tellement logique de faire une sauvegarde, qu'on se pose même pas la question de savoir qui nous a dit de le faire"* *"C'est sûr que les supports papiers, ça fait pas les calculs et il faut recommencer"*	*"Moi, j'ai été formé très jeune au niveau de l'aéronautique, où le comportement de non-divulgation d'une information, c'était inhérent à la profession, donc après, c'est quelque chose que l'on a en soi."* *"Je suis conscient que les informations que j'ai, je suis obligé de les garder (...) pour pas qu'elles tombent dans n'importe quelles mains".* *"C'est la société qui me fait vivre (...) et moi, j'ai un comportement moral en adéquation avec la fonction que j'ai"*	*"Je trouve que c'est pas bête parce que comme ça on peut faire jouer la concurrence, avoir de meilleurs prix sur les produits, c'est comme ça qu'on fait des économies, et qu'on fait marcher le commerce aussi".* *"C'est le dirigeant qui me l'a demandé au début (...) donc, c'est une méthode de travail qui m'a été apprise et voilà, je le fais comme si je fais une photocopie ou autre, c'est naturel. C'est devenu naturel."*
Aucun n'a été mentionné.	*"Il y a plein de choses que je ne sais pas faire en termes de sécurité"*	*"Et l'informatique, en plus pour des gens de notre génération, elle est venue en sus de l'activité qu'on avait. Et on n'a pas été formé comme les jeunes d'aujourd'hui"* Selon lui, il n'y a pas les moyens, ni en formation ni en matériel, d'avoir une bonne sécurité.	*"C'est compliqué parce qu'il faut que je sauvegarde pas tout le temps la même chose".* *"Il faut être relatif, ¼ d'heure c'est pas énorme non plus, mais ¼ d'heure de passé à ça, c'est pas ¼ d'heure passé sur un dossier"* *"Pour moi, personnellement, c'est la corvée."*

Tableau 3 : Extrait du verbatim des salariés : motivations et freins.

AUTEURS

Yves BARLETTE est professeur associé du Groupe Sup de Co Montpellier depuis 1989. Il est responsable de l'option « chargé d'affaires » du Master Management des Technologies de l'Information en partenariat avec l'IAE de Montpellier II. Il étudie la sécurité des SI (SSI) depuis l'année 2000. Dans ce cadre, il s'intéresse plus particulièrement aux comportements des acteurs en PME, ainsi qu'à l'adoption et à la mise en place des normes en SSI.

Adresse : Docteur en Sciences de Gestion, Professeur Associé, Groupe Sup de Co Montpellier – CEROM, 2300, avenue des Moulins, 34185 Montpellier Cedex 4, France
y.barlette@supco-montpellier.fr

Nabila BOUKEF CHARKI, enseignant-chercheur à l'ESDES (Ecole Supérieure de commerce & Management, Université Catholique de Lyon) et chercheur associée au DRM, CREPA, UMR CNRS n° 7088, Université Paris Dauphine. Docteur en Sciences de Gestion (Université Paris Dauphine). Ses recherches actuelles portent sur l'utilisation et les effets de la communication électronique.

Adresses :

- Enseignant-chercheur, ESDES, Université Catholique de Lyon, Université de Lyon, 23, place Carnot, 69286 Lyon Cedex 02, France
- Chercheur Associée, DRM CREPA, Centre de recherche en Management et Organisation, UMR CNRS n° 7088, Université Paris-Dauphine, Place du Maréchal de Lattre de Tassigny, 75775 Paris Cedex 16, France

nboukef@univ-catholyon.fr

Mohamed Hédi CHARKI, professeur associé à EDHEC Business School. Il a obtenu sa thèse en 2007 à l'Université Paris Dauphine. Il a été consultant dans une firme majeure de logiciels de gestion d'entreprise. Ses centres d'intérêts portent sur les places de marché électroniques, les enchères électroniques inversées et les relations inter-organisationnelles.

Adresse : Professor Associé, EDHEC Business School, 23, rue Delphin Petit, 59046 Lille, France
mohamed-hedi.charki@edhec.edu

Redouane EL AMRANI est Professeur des Systèmes d'Information à Reims Management School, France. Il est chercheur associé au laboratoire de recherche LEM de l'Université de Nantes. Ses recherches portent sur l'intégration des Systèmes d'Information, la transversalité, les systèmes ERP et Open Source et le changement organisationnel.

Adresse : Reims Management School, 59, rue Pierre Taittinger, 51100 Reims, France
redouane.elamrani@reims-ms.fr

Corinne JANICOT : Nos intérêts de recherche portent sur le management des connaissances, en particulier les stratégies de codification, et s'appuient sur l'étude de cas d'entreprises de services professionnels (secteur du conseil et de l'audit) et sur un observatoire des pratiques de gestion à partir d'un échantillon large et diversifié d'entreprises du Languedoc Roussillon. Nous nous intéressons également aux thématiques des progiciels de gestion intégrés (PGI) : nos travaux portent sur les relations entre les modélisations des processus type Business Process Management et les PGI.

Adresse : Maître de conférences, Université Montpellier II – IAE, Place Eugène Bataillon, 34095 Montpellier Cedex 5, France
corinne.janicot@univ-montp2.fr

Sophie MIGNON : Nos intérêts de recherche portent sur la pérennité des entreprises dont nous actualisons notre travail doctoral qui avait consisté à proposer une typologie, mettre en évidence des facteurs de pérennité et analyser le processus de pérennité organisationnelle et, sur le management des connaissances en nous centrant sur l'étude des stratégies de management des connaissances comme la stratégie de codification, mais également sur l'étude des dispositifs organisationnels et humains permettant de promouvoir le partage et le transfert.

Adresse : Maître de conférences, Université Montpellier II-IUT (Département GEA), 99, avenue d'Occitanie, 34296 Montpellier Cedex 5, France
tsmignon@club-internet.fr

Achevé d'imprimer sur les presses de l'Imprimerie BARNÉOUD
B.P. 44 - 53960 BONCHAMP-LÈS-LAVAL
Dépôt légal : mars 2009 - N° d'imprimeur : 902096
Imprimé en France