Protection du patrimoine informationnel des organisations

Comment expliquer la négligence des employés?

Chantal Desroches

Note de recherche no. 9

Chaire de recherche du Canada en sécurité identité technologie

Université de Montréal

Ce travail a été réalisé dans la cadre du cours CRI-6234, « Nouvelles technologies et crimes » (session d'hiver 2011), offert aux étudiants de la Maîtrise en Criminologie sous la direction du Professeur Benoît Dupont.

La Chaire de recherche du Canada en sécurité, identité et technologie de l'Université de Montréal mène des études sur les pratiques délinquantes associées au développement des technologies de l'information, ainsi que sur les mécanismes de contrôle et de régulation permettant d'assurer la sécurité des usagers.

Chantal Desroches
chantal.desroches@umontreal.ca

Prof. Benoît Dupont
Centre International de Criminologie Comparée (CICC)
Université de Montréal
CP 6128 Succursale Centre-Ville
Montréal QC H3C 3J7 - Canada
benoit.dupont@umontreal.ca
www.benoitdupont.net
Fax : +1-514-343-2269

Table des matières

INTRODUCTION

Chaque année, de nombreuses études[1] font état d'importantes pertes financières liées à la perte et au vol de données stratégiques au sein des organisations. En termes d'application de moyens de prévention et de politiques de sécurité, il semble que la bonne volonté des dirigeants, des directeurs de sécurité et des responsables des systèmes d'information ne soit pas suffisante pour réduire de façon significative le taux d'incidents répertoriés. En fait, cela ne constituerait que le point de départ à partir duquel la gestion du risque informationnel pourrait s'effectuer. Comme le précise Ghernaouti-Hélie (2007), une démarche de sécurité nécessite plusieurs étapes qui se définissent globalement par l'identification des risques, la spécification d'une politique de sécurité et la mise en place de mesures appropriées. Cependant, une fois les mesures de sécurité mises en place, comment s'assurer que les employés, principaux utilisateurs des systèmes d'information, respecteront les politiques qui leurs ont été imposées? Ce sont eux qui exploitent le système et qui, à travers différents mécanismes psychologiques, sociaux et économiques, prendront la décision de se conformer ou non. Si certains individus font preuve d'incompétence dans la manipulation d'informations stratégiques et confidentielles, à quoi peut-on attribuer le comportement négligent de nombreux autres employés qui, à première vue, ne semblent pas se soucier de protéger le patrimoine informationnel de l'organisation pour laquelle ils travaillent? Comme certains auteurs le soulignent, « L'employé est le premier vecteur potentiel d'informations stratégiques » (Faucon et Gaultier-Gaillard, 2010). Il est donc primordial de s'assurer que celui-ci, en plus de reconnaître la nature stratégique de l'information qui lui est confiée, adopte un comportement responsable en s'assurant qu'il se conforme à l'ensemble des politiques de sécurité de son organisation. Mais encore, qu'en est-il de l'employé consciencieux qui, pour des raisons qui nous paraissent incompréhensibles, ne respecte pas les politiques de sécurité auxquelles il est soumis? Considère-t-on ce cas comme de la négligence ou s'agit-il d'une problématique plus

[1] ASIS, Deloitte, Price Waterhouse Cooper, McAfee, Ponemon Institute

complexe qui se situe, en fait, au-delà de la simple volonté de l'individu? L'adoption de comportements négligents face à la sécurité de l'information, virtuelle ou tangible, sera donc l'élément central de cette note de recherche.[2]

L'objectif principal de ce travail consistera donc à explorer certaines avenues qui pourraient nous permettre d'améliorer notre compréhension du comportement des employés quant au respect des politiques de sécurité de leur organisation. En intégrant différentes perspectives à la compréhension du phénomène, il sera alors possible d'appréhender la problématique selon un angle nouveau. Plus spécifiquement, il sera question de mettre en lumière trois théories ayant contribuées à élaborer une piste d'explication aux comportements négligents des employés, lorsque vient le temps de se conformer aux politiques de sécurité qui leurs sont imposées. Ces théories sont les suivantes : la théorie de la motivation à la protection, la théorie de la dissuasion et la théorie du comportement planifié. Il ne s'agira pas ici, de déterminer laquelle est la plus appropriée pour aborder la problématique du comportement négligent des employés. Ce travail consistera plutôt à revisiter les travaux qui ont été fait à ce sujet d'une manière qui vise à en souligner les forces et les limites. Plus spécifiquement, les points qui auront été soulevés seront reconsidérés à travers le principe d'une gestion holistique de l'information, ce que Davenport nomme *Information Ecology* (Davenport, 1997).

MÉTHODOLOGIE

Comme il s'agit d'un travail relevant principalement d'une analyse critique de différents travaux, une méthodologie qualitative de type *analyse documentaire* a été privilégiée. Trois études empiriques ont été sélectionnées afin de constituer la base de cette réflexion:

[2] Notons que les comportements malveillants, qui constituent, en soi, une catégorie à part, ne seront pas considérés.

1. Herath, Tejaswini et H. Raghav Rao (2009). *Protection motivation and deterrence: a framework for security policy compliance in organisations.* Élaboration d'un modèle théorique à partir d'un sondage mené auprès de 312 employés de 78 organisations;
2. D'Arcy, John, Anat Hovav et Dennis Galleta (2009). *User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse : A Deterrence Approach.* Modèle théorique intégrant les éléments de la criminologie et de la psychologie sociale réalisé à partir de l'analyse de 269 utilisateurs de systèmes d'information répartis à travers huit organisations;
3. Siponen, Mikko, Seppo Pahnila et Adam Mahmood (2010). *Compliance With Information Security Policies: An Empirical Investigation.* Sondage effectué en Finlande auprès de quatre organisations représentant respectivement les secteurs suivants : technologies de l'information et des communications, sécurité de l'information, logistique et chaîne de supermarchés. Au total, 917 employés ont répondu au sondage.

Outre ces trois études, la consultation de différents textes théoriques et articles scientifiques s'est avérée nécessaire et ce, pour deux raisons : d'abord, pour clarifier la nature conceptuelle de chacune des théories exploitées et ensuite, pour intégrer les résultats à la logique argumentative préconisée par l'approche de l'écologie de l'information.

ÉTAT DES CONNAISSANCES

Les représentations du crime, qu'elles soient alimentées par les médias, par les pouvoirs politiques ou par les données fragmentaires que les organisations laissent filer, nous renvoient trop souvent à la cyber guerre : piratage massif ou espionnage économique initié par un état étranger. De plus en plus d'études nous dévoilent cependant une image différente et surtout moins *glamour* de la réalité à laquelle les organisations

doivent faire face : le comportement des employés. Un article de la revue *Scientific and Technical Information Processing*, publié en 2009, fait d'ailleurs état de diverses études publiques et privées qui se sont penchées sur les incidents liés à la sécurité de l'information. On y mentionne notamment, que les pertes les plus importantes rapportées au sein des organisations sont dues à la négligence et à l'incompétence des employés. L'auteur de cet article rapporte que le phénomène s'explique, entre autres, par le manque de formation et d'éducation en matière de sécurité de l'information. Il ajoute aussi que les employés ont peu conscience des risques auxquels ils sont exposés (Yelyakov, 2009). Par exemple, on fait mention d'un sondage[3] portant sur l'utilisation d'appareils électroniques mobiles. Celui-ci révèle que 78% des utilisateurs ont déjà perdu l'un de ces appareils alors qu'il contenait de l'information confidentielle non encryptée. Deux études (ASIS, 2006 et Sophos, 2010) rapportent d'ailleurs que le comportement des employés représente un enjeu majeur pour la protection du patrimoine informationnel des entreprises. La négligence, l'incompétence ou l'insouciance des employés face à la sécurité de l'information stratégique semblent donc relever d'une problématique généralisée à travers les organisations. L'analyse statistique réalisée par Dupont et Gagnon (2008) semble confirmer cette tendance. En effet, la distribution des causes d'incidents démontrent que le vol, la négligence et la perte représentent 71% des incidents répertoriés contre 22.7% pour le piratage.

Afin d'expliquer le phénomène mais surtout, afin d'apporter quelques piste de solutions, diverses approches ont été proposées à partir de cadres théoriques aussi variés que la théorie du choix rationnel, la théorie des jeux, la théorie de l'engagement organisationnel ou la théorie de l'échange social, pour ne nommer que celles-là. Conscientes de la problématique, les organisations cherchent maintenant de nouveaux moyens pour faire respecter les politiques de confidentialité à leurs employés; les méthodes conventionnelles ne semblent plus convenir à la réalité sociotechnologique avec laquelle celles-ci doivent composer (ASIS, 2011). Comme nous le savons, la

[3] Infowatch analytical center project: Mobile device security 2007.

prévention situationnelle est au cœur de nombreuses stratégies visant à protéger le patrimoine physique et virtuel des organisations. Faute de temps, de budget ou d'expertise, l'application de solutions toutes faites assez peu adaptées à la particularité de l'organisation et à l'environnement dans lequel elle évolue, constitue, dans bien des cas, le premier choix des gestionnaires en matière de résolution de problèmes (Clarke et Eck 2003, Berg 2008, Willison 2009). Sans nier l'efficacité des méthodes associées à la prévention situationnelle, il est toutefois pertinent d'aller un peu plus loin dans la démarche. Qui plus est, plusieurs des études empiriques répertoriées ont appuyé leurs conclusions à partir du point de vue des administrateurs et des dirigeants d'entreprises sans tenir compte de ce qu'ils appellent « le maillon faible », c'est-à-dire, les utilisateurs des systèmes d'information (Herath et Rao, 2009). Les études sélectionnées pour le présent travail nous offrent cette perspective. C'est en tentant de saisir certains éléments clés rendus manifestes à travers trois principales théories qu'il a été possible de rendre compte d'un problème sous-jacent dont il sera question plus tard. Comme nous utilisons une base comparative, seules les théories qui ont été employées par au moins deux des trois groupes seront considérées. Examinons d'abord la façon dont ces trois théories ont été exploitées. Nous verrons ensuite ce qu'elles peuvent nous apprendre sur le comportement des employés en matière de respect des politiques de sécurité.

THÉORIES : DÉFINITIONS ET APPLICATIONS

Théorie de la motivation à la protection

La théorie de la motivation à la protection (Rogers 1975, 1983) a été développée dans l'objectif de modéliser un cadre conceptuel permettant de mesurer les effets de la peur sur les attitudes et les comportements des individus. Initialement articulée afin de prédire les intentions comportementales en matière de protection personnelle, notamment dans le domaine de la santé, l'application de la théorie s'étend maintenant

aux questions environnementales ainsi qu'aux questions de sécurité. La PMT (Protection Motivation Theory) s'appuie principalement sur quatre facteurs :

1. la gravité de la menace perçue (par exemple, la perte ou le vol de données stratégiques est un problème grave qui touche de plus en plus d'organisations);
2. la vulnérabilité perçue (mon entreprise, par l'intermédiaire de mon poste de travail, pourrait faire l'objet d'une telle menace);
3. l'efficacité de la réponse (adhérer aux politiques de sécurité de mon organisation permet de réduire cette menace);
4. l'auto efficacité (j'ai les capacités nécessaires ou du moins, j'ai accès à un support technique lorsqu'il est question d'appliquer les politiques de sécurité de l'organisation pour laquelle je travaille).

Il est essentiel de préciser qu'un message basé sur les trois premiers facteurs doit être orienté soit, en fonction d'un comportement de détection soit, en fonction d'un comportement de prévention. Pour être efficace, le message qui vise le comportement de détection doit être faiblement anxiogène tandis que le message qui vise le comportement de prévention doit être fortement anxiogène. Dans les deux cas, « *La combinaison de ces trois variables cognitives (facteurs un à trois) éveillerait la motivation à la protection qui, à son tour, favoriserait l'adoption des recommandations proposées dans le message*.» (Girandola et al, 2003). Herath et Rao (2009) de même que Siponen, Pahnila et Mahmood (2010), ont utilisé la PMT dans le cadre de leurs recherches. Les résultats nous indiquent que la gravité de la menace perçue a un effet significatif sur l'intention de l'employé d'adhérer aux politiques de sécurité de son organisation. Toutefois, les résultats sont mitigés lorsqu'il est question de la vulnérabilité perçue (significatif seulement pour Siponen, Pahnila et Mahmood) et de l'efficacité de la réponse (significatif seulement pour Herath et Rao). Cela nous indique qu'en général, les employés sont conscients qu'il existe une menace et que celle-ci peut être très dommageable pour une organisation. Cependant, cette menace ne semble pas

avoir été intériorisée, du moins, pour les sujets de l'échantillon. Percevoir la gravité d'une menace est, en soi, insuffisant pour modifier la réponse cognitive et donc, pour engager un changement de comportement de la part de l'employé. Quant au quatrième facteur, les deux groupes de chercheurs parviennent à la conclusion qu'il y a un lien significatif entre l'auto-efficacité et l'intention d'adhérer aux politiques de sécurité de l'organisation. À la lumière des premières constations, il est toutefois légitime de se demander si ce dernier facteur est encore pertinent.

Théorie générale de la dissuasion

Parmi les trois études sélectionnées, celle de D'Arcy, Hovav et Galetta (2009) fait de la théorie générale de la dissuasion son modèle théorique central. Herath et Rao (2009) la considère comme un complément à la théorie de la motivation à la protection alors que Siponen, Pahnila et Mahmood (2010) l'utilise comme modèle comparatif. Avant de présenter leurs hypothèses et résultats, revenons sur les prémisses de base de cette théorie. La théorie générale de la dissuasion repose sur l'hypothèse de base qu'un individu sera dissuadé de commettre un crime s'il perçoit les sanctions comme étant sévères, certaines et rapidement applicables (William et Hawkins 1986). Le concept même du crime peut toutefois prendre une définition plus large. Les auteurs considèrent en effet que dès qu'un comportement est jugé inacceptable par l'organisation, une sanction peut s'appliquer. Suivant cette logique, les hypothèses suivantes ont été avancées:

1. la sévérité de la sanction aura un effet positif sur l'intention de se conformer aux politiques de sécurité;
2. la certitude d'être détecté aura un effet positif sur l'intention de se conformer aux politiques de sécurité;

3. La promptitude (célérité) des actions de détection et d'application de la sanction aura un effet positif sur l'intention de se conformer aux politiques de sécurité. (Mesurée uniquement par Siponen, Pahnila et Mahmood)

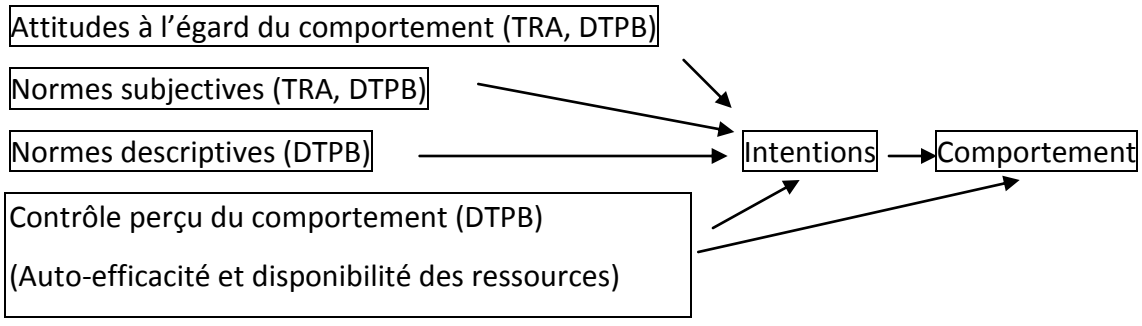
Il est important de préciser que chacun de ces trois points implique la notion de perception. Par conséquent, nous pouvons présumer que même si les éléments de dissuasion sont clairement expliqués et uniformément diffusés à travers l'organisation, la perception de la sanction, de par sa nature subjective, sera issue d'un processus cognitif individuel.

Si la méthodologie par sondage semble appropriée pour étudier ce processus, Williams et Hawkins (1986) suggèrent toutefois de « recréer artificiellement » les situations en introduisant une distinction précise entre les différents « délits » et leurs sanctions respectives (p.567). Si on cherche à mesurer la perception à partir d'éléments mal définis ou portant à confusion, on réduit de façon substantielle la validité de la mesure. Nous nous retrouvons donc avec trois critères à respecter : a) présenter aux répondants des scénarios représentatifs de la réalité, b) préciser les délits, c) préciser les sanctions pour chaque délit. Même si les trois études sélectionnées ont utilisé des approches relativement différentes, notamment en ce qui a trait aux questionnaires et aux modèles d'analyse, il est étrange de constater qu'aucune n'a respecté intégralement les trois critères. Qui plus est, les résultats démontrent certaines contradictions. Herath et Rao (2009) obtiennent un effet significatif entre la certitude d'être détecté et l'intention de respecter les politiques de sécurité alors que la sévérité aurait un impact négatif. D'Arcy, Hovav et Galletta (2009) concluent au contraire, que la sévérité des sanctions a un effet beaucoup plus significatif que la certitude d'être détecté. Quant à Siponen, Panhila et Mahmood (2010), leurs résultats suggèrent que tant la sévérité de la sanction que la certitude d'être détecté auraient un impact significatif sur l'intention de respecter les politiques de sécurité de l'organisation. Ceux-ci précisent également que la détection et la sanction devraient s'effectuer rapidement pour produire l'effet

escompté. Pour ce qui est des deux études précédentes, ce dernier élément (la célérité) n'a pas été pris en compte. Comme nous faisons face à des résultats relativement contradictoires et que le critère de célérité n'a été mesuré que dans une seule des trois études, il faut demeurer prudent quant aux conclusions que l'on peut tirer de l'effet de la sanction sur l'intention des employés d'adhérer aux politiques de sécurité de leur organisation.

Théorie du comportement planifié

Examinons maintenant la théorie du comportement planifié, théorie qui a été exploitée différemment par deux groupes de chercheurs : Siponen, Panhila et Mahmood (2010) ainsi que Herath et Rao (2009). Les premiers ont préféré utiliser la théorie de l'action raisonnée ou TRA (Ajzen et Fishbein 1980). Celle-ci est considérée comme la version originale de la Théorie du comportement planifié (Ajzen 1991). Exprimée simplement, cette théorie stipule que les intentions, issues d'attitudes et de normes subjectives, constituent un bon indicateur du comportement des individus pour une situation donnée. Quant à Herath et Rao, ceux-ci ont choisi de concevoir l'intégralité de leur modèle à partir des préceptes développés par Taylor-Todd (Decomposed Theory of Planned Behavior ou DTPB). Il s'agit en fait de la théorie du comportement planifié mais adaptée au contexte des technologies de l'information. Nous retrouvons au sein de cette version, deux éléments supplémentaires : les normes descriptives et le contrôle perçu du comportement. Le schéma suivant illustre les relations qui prévalent à l'intérieur des deux modèles (TRA et DTPB).



Qu'il s'agisse de TRA (Theory of Reasonned Action) ou de DTPB (Decomposed Theory of Planned Behavior), l'objectif est de rendre compte des facteurs qui permettent de prédire les intentions des employés d'adhérer aux politiques de sécurité de leur organisation. Le meilleur prédicteur du comportement serait donc l'intention. Suivant cette logique, les hypothèses suivantes ont été posées:

1. Attitude à l'égard du comportement : une attitude positive face au respect des politiques de sécurité devrait suggérer une intention de se conformer aux dites politiques;
2. Les pressions sociales : les normes subjectives (comment mes pairs/supérieurs s'attendent à ce que je me comporte) et les normes descriptives (comment mes pairs/supérieurs se comportent), devraient avoir une influence positive sur l'intention d'adhérer aux politiques de sécurité;
3. Contrôle perçu du comportement: l'employé croit qu'il possède les habiletés adéquates et les ressources suffisantes pour adhérer aux politiques de sécurité de son organisation (similaire à l'auto-efficacité de la PMT).

Comme nous l'avons vu pour la Théorie de la Motivation à la Protection, l'auto-efficacité tout comme la disponibilité des ressources (humaines et techniques) jouent un rôle essentiel lorsqu'il est question de se conformer aux politiques de sécurité d'une organisation. Les pressions sociales semblent aussi avoir un impact important sur l'intention de se conformer. Herath et Rao tout comme Siponen, Pahnila et Mahmood, obtiennent des résultats similaires quant aux normes subjectives. Il s'avère en effet, que la façon dont un employé perçoit le comportement de ses pairs (collègues, supérieurs, informaticiens) influence significativement l'intention de celui-ci de se conformer ou non aux politiques de sécurité qui lui sont imposées. En résumé, on affirme que certains facteurs (attitude favorable, pressions sociales, contrôle perçu du comportement) modulent l'intention d'adhérer aux politiques de sécurité et que cette intention, délibérée et planifiée, présume l'action.

CRITIQUES ET LIMITES

Le caractère intentionnel

D'abord, l'intention suppose un acte volontaire (Parent, 2007)[4]. Les trois études et ce, peu importe la théorie exploitée ou les résultats obtenus, se sont basées sur un présupposé manifeste : l'employé qui n'adhère pas aux politiques de sécurité et donc, qui menace le patrimoine informationnel de son organisation, le fait de façon intentionnel. Pourtant, bon nombre d'études provenant de firmes privées telles que Sophos, PWC, Deloitte ou ASIS aborde la notion d'incident, d'erreur ou d'inadvertance. Même la négligence et l'incompétence résultent, la plupart du temps, d'une faute non intentionnelle se traduisant par un manque d'attention, de vigilance ou d'application. Seule l'étude de D'Arcy, Hovav et Galletta annoncent, dès les premières lignes, qu'ils feront référence aux comportements intentionnels. Aucune distinction claire n'est proposée par les deux autres groupes de chercheurs. Pourtant, leurs cadres théoriques visent, de façon non équivoque, à mesurer les intentions des employés d'adhérer aux politiques de sécurité de leur organisation. On prend donc pour acquis le caractère intentionnel de l'acte. Par conséquent, on suppose que tout comportement qui dévie de la norme imposée est réputé avoir été réalisé volontairement. Et s'il s'agissait, pour la plupart, d'employés honnêtes qui ont l'intention d'adhérer mais qui, pour une raison ou pour une autre, ne le feraient pas? Le deuxième constat pourrait peut-être nous offrir une piste de réponse.

L'approche « Top-Down »

Les auteurs sont tous d'accord pour affirmer que la clé du succès, lorsqu'il est question d'amener les employés à respecter les politiques de sécurité, réside dans le principe de sensibilisation. Les employés doivent être éduqués, formés et sensibilisés aux politiques

[4] Ici, nous faisons généralement référence aux cas non définis par le législateur.

de sécurité que l'organisation impose dans le but de protéger son patrimoine informationnel. Ce processus se traduit par des activités de persuasion parfois intensives auprès des employés grâce à une série de méthodes aussi variées les unes que les autres (affiches, messages électroniques, campagnes de sensibilisation, programmes de formation). Les auteurs se sont donc demandé, à l'aide de théories comportementales, comment serait-t-il possible d'influencer ce processus de persuasion. L'objectif de leur recherche consistait donc à découvrir une façon qui permettrait de modifier un comportement afin de le rendre conforme aux normes imposées. Il existe toutefois une limite considérable dont il faut tenir compte : le comportement évalué a été extrait de son contexte. Plus spécifiquement, les tâches et les objectifs de productivité liés à chaque poste de travail (sous-groupe ou département) n'ont pas été considérés.

Les politiques de sécurité sont créées par les administrateurs de systèmes d'information, les responsables de la sécurité et les gestionnaires. Ceux-ci assument que leurs politiques de sécurité, une fois associées à certaines méthodes (provenant des recherches empiriques précédemment mentionnées par exemple) seront assimilées et respectées par les usagers et ce, sans même avoir tenu compte de leurs points de vue. C'est ce qu'on appelle « *digital divide* » (Albrechtsen, Hovden, 2009). Il s'agit en fait d'un problème qui découle du manque d'interaction entre les responsables de la sécurité de l'information et les usagers. Ce manque d'interaction conduit les gestionnaires à créer des pratiques et des politiques de sécurité qui sont parfois totalement déconnectées de la réalité des usagers. Que les employés soient formés et éduqués à des politiques de sécurité facilement compréhensibles ne changent rien au problème puisqu'une partie de ce dernier est issu de la communication unidirectionnelle qui prévaut dans une majorité d'organisation; le « Top-down management ». Ce type de gestion de la sécurité de l'information place l'employé dans une situation inconfortable où il doit parfois choisir entre le respect des politiques de

sécurité et la productivité de son entreprise (Christopher Burgess, 2009)[5]. De récentes études, réalisées respectivement par *Deloitte* (2010) et *PricewaterhouseCoopers* (2011) font d'ailleurs état de la nécessité de faire converger les objectifs de sécurité de l'information aux objectifs de l'organisation; cette stratégie devant idéalement être accomplie à partir de la contribution de chaque centre d'activités ou département. En adoptant une telle stratégie, non seulement les employés évitent de se heurter à une situation que nous pourrions qualifier de « jeu à somme nulle » mais encore, l'organisation est en mesure d'évaluer concrètement l'impact des politiques de sécurité mises en place.

La connaissance de ce qui doit être protégé

Abordons maintenant le dernier constat; constat qui ne s'applique pas qu'aux études sélectionnées pour le présent travail. D'abord, on s'est demandé si les politiques de sécurité des organisations étaient jugées adéquates par rapport aux dangers qui les menaçaient. Ensuite, on s'est penché sur les raisons pour lesquelles certains employés n'adhéraient pas aux politiques de sécurité qui leurs étaient imposées. Nous avons donc identifié la menace et élaboré les moyens pour en réduire les risques. Mais sait-on vraiment ce qui doit être protégé? Abordons la question autrement; est-ce qu'un employé est en mesure d'identifier ce qui constitue le patrimoine informationnel de son entreprise? Il semble que ce ne soit pas toujours le cas. Une enquête sur la sécurité des documents menée en 2006 par Canon Europe-ICM révèle en effet que « *Deux employés sur dix pensent qu'il est admissible de lire des documents sensibles laissés sur une imprimante et 46% des employés affirment avoir déjà parlé d'informations confidentielles en dehors du bureau*. » Aussi, selon une étude portant sur la sécurité informatique et la valeur des écrits au travail, « *la plupart des documents manipulés, reçus, envoyés, ne valent pas aux yeux de leurs lecteurs ou auteurs l'arsenal de*

[5] Commentaire recueilli à partir du site : http://www.networksecurityedge.com/content/effective-security-policy-messaging-important. Christopher Burgess est conseiller senior pour la sécurité chez Cisco. Il était auparavant Conseiller senior pour la sécurité nationale.

précautions qu'on voudrait bien leur prêter pour empêcher qu'ils soient volés ou perdus. » (Denis, 2009). Suite aux entretiens effectués dans le cadre de sa recherche, Denis constate que tant qu'un document n'est pas qualifié de stratégique ou de confidentiel, sa valeur reste floue aux yeux des usagers. D'une part, les répondants croient que les données brutes sont inutiles et sans valeur pour les concurrents puisqu'elles sont dépouillées de leurs sens (du contexte dans lequel elles ont été produites). D'autre part, on minimise la perte de documents en prétextant leur duplication à travers l'organisation. En prétendant une attribution uniforme de la valeur de l'information qui doit être protégée, on omet une étape essentielle du processus de résolution de problème. Par conséquent, l'atteinte des objectifs liés à la sécurité de l'information risque de souffrir de cette lacune.

UNE APPROCHE INTÉGRÉE : *INFORMATION ECOLOGY*[6]

Force est de constater que la problématique liée à la négligence des employés devient beaucoup plus complexe lorsque nous considérons l'intégralité du contexte organisationnel. L'une des critiques adressée à l'approche de la prévention situationnelle fait d'ailleurs état de cette difficulté. À travers ces trois constats, il a été possible de dégager une tendance qui pourrait se traduire par une absence de concertation entre les acteurs impliqués dans la sécurité de l'information. Il ne s'agit plus uniquement de suggérer une collaboration étroite entre les responsables de la sécurité et les administrateurs de systèmes d'information mais bien d'inclure la perspective des usagers dans l'élaboration des politiques de sécurité. Le principe de l'écologie de l'information repose sur une métaphore qui suggère de modéliser l'environnement informationnel à partir des individus qui gravitent à l'intérieur de cet environnement; ce que Davenport décrit comme une gestion holistique de l'information. Selon cette approche, la gestion de l'information doit être considérée comme un procédé imparfait et changeant qui implique de connaître la façon dont les

[6] Davenport (1997)

membres de l'organisation utilisent « vraiment » l'information. L'auteur suggère également qu'il faut voir la technologie comme un outil utilisé par les employés pour les aider à accomplir leurs tâches et non pour la compliquer. Loin de nier qu'il est essentiel de modifier les comportements des employés à l'égard de la sécurité de l'information, Davenport souligne cependant que l'application de telles mesures nécessite l'établissement de processus de communication entre spécialistes, usagers et gestionnaires. Si l'écologie de l'information vise d'abord à développer une stratégie globale de la gestion informationnelle, elle doit aussi prendre racine à tous les niveaux de l'organisation. « Think globally, but act locally »[7] illustre parfaitement ce que Davenport propose. Les moyens qu'il suggère pour mettre en œuvre un tel projet s'inscrivent dans ce qu'il nomme « la gestion du comportement informationnel ». En voici les principaux éléments :

- Communiquer l'utilité et la valeur de l'information;
- Clarifier les stratégies et objectifs de l'organisation en matière de gestion de l'information;
- Identifier les besoins et compétences informationnelles;
- Mettre l'emphase sur une gestion spécifique du contenu informationnel;
- Assigner des responsabilités en matière de gestion du comportement informationnel et intégrer ces responsabilités à la structure organisationnelle;
- Créer un comité ou un réseau dont la tâche spécifique sera de discuter des questions relatives à la gestion du comportement informationnel;
- Éduquer les employés quant au comportement à adopter;
- Soulever les points qui constituent des inquiétudes quant au comportement à adopter en matière de gestion informationnelle et en discuter avec tous les employés concernés.[8]

[7] Christopher Burgess, 2009. Guest opinion on Network Security Edge
http://www.networksecurityedge.com/content/effective-security-policy-messaging-important
[8] Adapté de Davenport (1997)

Ces propositions ne viennent en rien contredire les conclusions qui ont été apportées par les études précédentes. Elles comblent plutôt les limites qui ont été soulevées : le caractère intentionnel du comportement, l'approche « Top-down management» et la connaissance de ce qui doit être protégé. Les propos de l'auteur sont d'ailleurs éloquent à ce sujet : « *When individual employees must determine on their own how to identify, share, and otherwise behave toward information, it's unlikely they'll make the best use of what is undeniably and important competitive resource* » (Davenport, 1997, p.106).

CONCLUSION

Nous avons pu constater que la négligence des employés face à la sécurité de l'information découle d'une problématique complexe qui nécessite un examen approfondi de la gestion informationnelle préconisée au sein de chaque organisation. Bien qu'encore très utiles, les méthodes conventionnelles de prévention ne sont plus suffisantes pour faire face à la situation. Conscient de ce problème, certains chercheurs se sont tournés vers les théories comportementales d'une part, pour tenter d'expliquer la conduite des employés et d'autre part, pour apporter quelques pistes de solutions. Un examen des études empiriques sélectionnées spécifiquement pour ce travail a toutefois fait émerger trois éléments qui pourraient sans doute faciliter l'atteinte des objectifs anticipés par la sécurité de l'information. Cependant, pour une raison qui nous échappe, ces éléments ont été soustraits de l'équation. En voici un résumé : d'abord, on présuppose que l'employé qui n'adhère pas aux politiques de sécurité de son organisation le fait de façon intentionnelle; ensuite, on applique la technique du « top-down management » en présumant une adhésion quasi-automatique aux politiques de sécurité; finalement, on prend pour acquis que l'employé est en mesure d'identifier ce qui constitue le patrimoine informationnel de son organisation. Ne pas considérer ces éléments nous porte à croire que le problème a été, initialement, mal défini. Par conséquent, la mise en application des politiques de sécurité s'en est trouvée

directement compromise ou du moins, c'est ce qui est sous-entendu par les conclusions de diverses études qui ont pu être consultées.

L'approche préconisée par l'écologie de l'information n'est pas nouvelle en soi mais il semble que sa mise en application tarde à se faire sentir au sein des organisations. Les récents sondages réalisés par certaines firmes spécialisées telles que *Deloitte* ou *PricewaterhouseCoopers* laissent toutefois transparaitre cette nécessité d'une gestion holistique de l'information à partir d'une perspective qui vise maintenant la sécurité du patrimoine informationnel. Cette transformation du modèle traditionnel de gestion nous permet de supposer que les principes développés au sein de l'écologie de l'information peuvent s'adapter aisément aux objectifs poursuivis par la sécurité des organisations.

Les ouvrages théoriques proposant une gestion holistique de l'information, une implication de tous les acteurs de l'organisation et une communication multidirectionnelle à propos de la gestion des risques informationnels se multiplient. Pourtant, les études empiriques disponibles ne permettent pas encore de mesurer, de manière concrète, la portée de ce type de « gouvernance de la sécurité » (Ghernaouti-Hélie, 2007). Voilà peut-être un objet de réflexion sur lequel il serait pertinent de se pencher.

RÉFÉRENCES

Albrechtsen E. et J. Hovden (2009). The information security digital divide between information security managers and users. Computer and Security, vol. 28 (2009) pp. 476-490

Bonardi et al. (2003). Psychologie sociale appliquée: Économie, Médias, Nouvelles technologies. Éditions *In Press*, Paris.

D'Arcy, J., A Hovav and D. Galletta (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, vol. 20, no.1, march 2009, pp. 79-98

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

Denis, Jérôme (2009). Sécurité informatique et valeur des écrits au travail. *Semen, Revue de sémio-linguistique des textes et discours*. Vol.28, pp. 85-100
URL : http://semen.revues.org/8732 Consulté le 16 mars 2011.

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

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

Girandola and Al. (2003). Prévention, détection et traitement de l'information persuasive en situation de peur. Revue Canadienne des Sciences du Comportement, vol. 35, no.3, (2003), pp. 197-209

Foryst, C. A. (2010). Rethinking National Security Strategy Priorities. *International Journal of Intelligence and CounterIntelligence,* 23: 3, 399 — 425

Herath T. and H. Raghav Rao (2010). Control mechanisms in information security: a principal agent perspective. Intelligence Journal of Business, Governance and Ethics, vol. 5, nos.1/2, 2010

Herath T. and H. Raghav Rao (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, vol. 18, pp. 106-125

Huang, D.-L., P.-L. Rau and G. Salvendy (2010). Perception of Information Security. *Behaviour & Information Technology* Vol. 29, No. 3, May–June 2010, 221–232

Jervis, Robert (1979). Review: Deterrence Theory Revisited. *World Politics*, Vol. 31, No. 2 (Jan., 1979), pp. 289-324. Cambridge University Press.

Kramer S., P. Carayon et J. Clem (2009). Human and organisational factors in computer and information security: Pathways to vulnerabilities. *Computer and Security*, vol. 28, (2009), pp. 509-520

Parent, Hugues (2007). Traité de droit criminel, 2e édition. *Édition Thémis*, Faculté de Droit, Université de Montréal.

Rittenburg, T. L., S.R. Valentine and J.B. Faircloth (2007). An Ethical Decision-Making Framework for Competitor Intelligence Gathering. *Journal of Business Ethics* (2007) Vol. 70, pp. 235–245

Williams, Kirk R. and Richard Hawkins (1986). Perceptual Research on General Deterrence: A Critical Review. *Law & Society Review*, Vol. 20, No. 4 (1986), pp. 545-572

Yelyakov, Akopyan (2009). Cybercrimes in the information structure. *Scientific and Technical Information Processing*, vol. 36, no. 6, 2009

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

Financial Services Global Security Study: The faceless threat. *Deloitte* (2010)

Global State of Information Security Survey 2011. *PricewaterhouseCoopers, CIO Magazine and CSO Magazine*.

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

The Value of Corporate Secrets. How Compliance and collaboration affect enterprise perception of risk. March 2010. Forrester Research. *Forrester Consulting*.

Trends in Proprietary Information Loss. Survey Report, 2007. *ASIS International*