Vol et fuites de données :

Le cas interne

Audrey Asseman

Note de recherche no. 3

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'automne 2009), 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.

Audrey Asseman
audrey.asseman@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

L'étude de la criminalité économique est l'objet d'un intérêt cyclique qui ne correspond pourtant pas à une réalité quotidienne où le lieu de travail fait l'objet d'une multitude de délits. L'un de ces délits, le vol, est courant et se perpétue depuis (presque) toujours. Il est intéressant de ce pencher sur le vol en interne, car il va souvent à l'encontre de ce qui caractérise couramment la délinquance : la pauvreté, le style de vie festif… alors qu'ici il s'agit d'individus menant une vie toute à fait ordinaire. De plus, l'origine positiviste de la criminologie dont Lombroso est une des figure de ce courant identifie un criminel sous des traits de personnalités inadaptés alors que l'employé lui est parfaitement adapté au milieu et aux normes, voire même dispose de facultés supérieures. Il est donc pertinent de vouloir comprendre cette déviance, car elle est pratiquée partout et par tous, mais à des degrés et des moyens différents. Par ailleurs, bien que ce phénomène soit répandu, les données disponibles sont rares et donc font l'objet d'un chiffre noir important.

À l'inverse des pertes internes, la menace externe a été davantage traitée dans la littérature. Les organisations sont donc de mieux en mieux protégées face à celle-ci. En revanche, le côté interne a été quelque peu mis de côté face à la peur du pirate, nous tenterons donc dans ce travail d'éclaircir les connaissances sur cette problématique de vol et de perte de manière interne. Les nouvelles médiatisées, bien qu'anecdotiques (on se souviendra du cas de la firme Coca-Cola qui s'était fait voler la recette de sa fameuse boisson par une secrétaire pour la vendre à son concurrent Pepsi. On pense aussi a l'ancien scientifique de la société DuPont qui est partie avec des documents commerciaux d'une valeur de 400 millions de dollars après s'être fait engagé dans une société rivale) n'enlève pas moins à la réalité de la menace qu'elle soit malveillante ou par négligence dont les conséquences sont souvent omises et qui touche autant les organisations publiques que privées.

Le présent travail a pour objectif de cerner davantage la perte de données en interne afin d'en obtenir une vision plus réaliste et sans être exhaustive, plus complète. Nous commencerons donc par définir les termes de notre sujet, par rendre compte de l'état actuel ainsi que des conséquences. Puis nous examinerons les aspects facilitateurs de ces pertes et enfin nous terminerons sur quelques propositions d'éléments de prévention.

LA PERTE DE DONNÉES : DÉFINITIONS

La perte de données en interne peut revêtir des formes multiples tant du point de vue de la cible que des moyens. On comprend généralement sous le terme de donnée, l'ensemble des informations qui sont la propriété intellectuelle de l'organisation ainsi que les informations qu'elle dispose sur ses clients ou ses partenaires. Il s'agit entre autres des renseignements personnels des clients, des employés, les contrats, les innovations, les secrets commerciaux, procédures techniques, documents de travail… Face à cette diversité de cibles, différents types de perte s'exercent. Ici nous détaillerons la négligence, l'espionnage industriel et le vol de données en interne. Ce dernier sera expliqué notamment par les définitions générales du vol en interne, qui comporte les biens, car la littérature portée sur le vol de données exclusivement est moins bien étoffée.

La fuite de données

La fuite d'information est traditionnellement comprise comme accidentelle. Elle résulte de la négligence des employés qui dans le cadre de leur travail ou en dehors commettent des erreurs non intentionnelles de divulgation d'information. Caractéristique de l'erreur humaine, elle s'exprime par l'oubli d'un cellulaire ou d'un ordinateur portable dans un aéroport, par la discussion entre collègues au restaurant du coin de la rue, par l'envoi d'un message électronique à un mauvais destinataire. Il n'existe pas de définition connue, car elle est plutôt définie par opposition au vol de donnée en interne qui se caractérise par la malveillance, par opposition à l'acte de vol délibéré. On peut noter ici que, contrairement aux deux prochaines formes de perte, celle-ci n'est pas criminelle bien qu'elle peut avoir les mêmes conséquences si les données sont récupérés et utilisées illégalement.

L'espionnage industriel

L'espionnage industriel est défini selon Payne (1971) comme « *l'homme ou la femme qui d'une manière clandestine, s'approprie des renseignements confidentiels et les revends à l'insu de leurs propriétaires. En procédant ainsi, l'espion agit contre les intérêts du propriétaire, lui dérobant la propriété de son travail, de ses recherches et de son avance technique pour faire bénéficier quelqu'un d'autre* ». On peut s'étonner de parler d'espionnage lorsqu'on aborde le cas interne des organisations, mais nous devons tout de même l'évoquer car l'espionnage, bien que dirigé par une organisation externe, souvent concurrente, peut revêtir un aspect interne. Il s'agit de deux catégories d'espions sur les trois que proposent Payne (1971) : l'« *opportuniste* » qui par son travail et sa fonction lui donne accès à une information qu'il va proposer de revendre à une compagnie rivale et le « *stringer* » qui à l'aide d'un correspondant de l'organisation va obtenir les informations qu'il souhaite. Sans tomber dans la suspicion paranoïaque, il faut être conscient que l'espionnage n'est pas exclusivement une menace externe et que les employés peuvent être utilisés. Plus récemment, Dupré (2001) définit l'espionnage économique comme « *le fait pour une personne physique ou morale, de rechercher dans un but économique, pour soi ou pour autrui, de manière illégitime – c'est-à-dire le plus souvent à l'insu et contre le gré de son détenteur – des informations techniques ou de toute nature lorsque ces informations présentent une valeur, même potentielle, dont la divulgation serait de nature à nuire aux intérêts essentiels de ce dernier* ». Les « Trade secrets » ou secrets commerciaux sont définis selon Fraumann (1997) comme « *toutes les formes et types d'informations financières, commerciales,*

scientifiques, techniques, économiques ou ingénieries qui inclut les patrons, les plans, les compilations, formules, designs, méthodes, prototypes, techniques, procédures, codes, programmes… tangibles ou intangibles et qui peuvent être stockés de façon mémorisée physiquement, électronique, graphique, photo ou écrite ». L'avantage d'une telle définition est qu'elle détaille l'ensemble des cas de figure possibles et reconnait aux données une valeur appartenant à l'entreprise. Selon ce même auteur, parmi les méthodes intrusives possibles, l'accès au personnel employé dans l'environnement protégé est celle qui peut se comprendre à la fois comme une menace externe et interne puisque les quatre modalités de cette méthode concernent l'intérieur de l'entreprise. La première est d'engager un employé qui possède les renseignements désirés de la société cible. La seconde est d'introduire un agent dans l'entreprise cible, dont l'identité est cachée dans le but de compromettre les employés clés, consulter les bases de données, intercepter les communications afin d'obtenir les informations confidentielles. La troisième consiste à réaliser un faux recrutement pour obtenir des employés qu'ils parlent de leur entreprise. Enfin, la dernière consiste à corrompre, acheter un employé ou un fournisseur. Ainsi comme nous pouvons le constater, l'espionnage industriel revêt des formes qui s'exercent au sein de l'organisation ou qui utilise les individus en faisant partie.

Le vol en interne

Le cas du vol interne est davantage traité dans la littérature, il existe donc un panel de définitions différentes. On parlera de vol interne, de vol par les employés, ou encore de fraude. La criminologie américaine distingue plusieurs catégories du « White-collar crime » : *corporate crime* c'est-à-dire les crimes commis par les personnes qui ont une place élevée dans la hiérarchie de l'entreprise et *occupational crime* qui concerne spécifiquement la criminalité des salariés (Bonnet, 2007 & 2008). Quel que soit le terme donné, le vol interne se produit à tous les échelons de l'organisation. Une des définitions les plus connues est celle de Hollinger et Clark (1983) : *« By employee theft, we specially mean the unauthorized taking, control, or transfer or money and/or property of the formal work organization that is perpetrated by an employee during the course of occupational activity »*. Dans cette définition, on oriente plus l'intérêt sur les biens ou l'argent et on cantonne le vol au moment où l'individu est dans son activité. Or pour le vol de données, beaucoup de vols s'effectuent au moment de quitter l'emploi. La définition sur laquelle nous baserons notre étude, car plus complète, est celle de Greenberg (1997) : « *Employee theft is defined as any unauthorized appropriation of company property by employees either one's own use or for sale to another. It includes, but is not limited to, the removal of products, supplies, material, funds, data, information, or intellectual property* » (p.86).

Il est important de noter que d'un point de vue juridique, il n'existe pas de « vol d'information » à proprement parler (Dupré, 2001 ; Barel, 2009), car comme le précise la définition donnée précédemment, il faut que le geste ne soit pas autorisé, or l'accès à l'information est donné par l'employeur à l'employé dans le cadre de son travail. On peut alors évoquer l'abus de confiance (Gallet, 2005). Cette idée est exprimée par Felson (2002) en terme de « crime d'accès spécialisé » (crimes of specialized access) qu'il explique comme « *a criminal act commited by abusing one's job or profession to gain specific access to a crime target* » (p.95). La difficulté juridique que pose cette accessibilité est en partie une des raisons du faible taux de report de la part des organisations. Pour pallier à l'inexistence du « vol interne d'information », l'ACFE (Association of Certified Fraud Examiner) utilise l'expression « occupational fraud » pour

caractériser la fraude dans le milieu de travail et la définit comme « *l'utilisation par une personne de son activité professionnelle pour s'enrichir personnellement par le détournement volontaire des ressources ou des actifs de son employeur* ». À travers cette dernière définition on insiste sur le caractère délibéré, l'intention contrairement à l'erreur qui peut s'appliquer sur toute chose qui représente une valeur propriété de l'organisation.

AMPLEUR DU PHÉNOMÈNE

Qu'est-ce que cela représente?

Une étude réalisée par Rotman-TELUS (2009) sur 300 professionnels de la sécurité et des technologies d'informations au Canada a montré une augmentation des menaces depuis la crise économique de 2008. Les cinq types de brèches ayant eu les augmentations les plus rapides sont : 1. L'accès non-autorisé à des informations par des employés (+ 112%) ; 2. Ordinateurs compromis (Botnet; +88%); 3. Fraude financière (+88%) ; 4. Vol d'informations propriété de l'entreprise (+75%) ; 5. Vol d'ordinateurs portables et de cellulaire (+58%). Il apparait donc clairement que la menace interne est de plus en plus vigoureuse notamment depuis la crise. Dans cette même étude, qui compare le Canada aux États-Unis, entre 2008 et 2009 les brèches relatives à des activités internes étaient de 17% pour le Canada et de 60% pour leur voisin. L'année suivante, elles ont augmenté de 36% alors qu'elles ont diminué de 44% aux États-Unis, ce qui peut démontrer d'une conscientisation de la part des firmes américaines. Face à l'augmentation des menaces, les professionnels canadiens interrogés disent avoir réduit de 10% leur budget attribué à la sécurité des données due à la crise. De plus, l'augmentation de personnel étant rare, les technologies de prévention et contrôle n'ont pas été déployées.

CyberArk (2008) a interrogé 600 employés en Angleterre, Hollande et États-Unis à travers un sondage auto révélé sur le vol d'information en interne. Les résultats montrent que 25% des employés anglais, 52% des employés américains et 31% des employés hollandais partiraient avec des informations sur les clients et les contacts. Toujours selon cette étude, excepté les Anglais (29%), les Américains et les Hollandais reconnaissent qu'il est facile de voler des informations importantes de l'entreprise (62% et 54%). À la question sur le moyen que les employés utiliseraient pour partir avec des informations, la réponse qui arrive en première position pour tous les répondants est l'utilisation d'une clé USB.

L'étude réalisée par Verizon (2009) sur 90 brèches confirmées en 2008 donne le chiffre impressionnant de 285 millions de données compromises. Parmi ces brèches, 20% sont causés par les employés, mais malgré cette faible proportion, elles sont plus dommageables que les brèches externes. De plus, les brèches internes sont pour les deux tiers d'origine malveillante et le tiers restant de la négligence. Par ailleurs, selon le Clusif (2009), 80% de la malveillance serait interne. Il y a donc des écarts importants entre les études mais qui attestent toutes de l'importance du phénomène de la fuite de données en interne. Malgré ces chiffres, seulement 15% des entreprises analysent le problème de la perte de données en interne. De plus, sur ces 15%, lorsque des analyses sont faites 45% les trouvent incomplètes et 29% superficielles (Ponemon, 2009).

Qui sont les « voleurs » internes?

Selon l'étude réalisée par Ponemon Institute (2009), 59% des employés volent les données quand ils partent de la société et 79% d'entre eux admettent qu'ils n'avaient pas la permission de leur ancien employeur. Même lorsque les 16% disent avoir eu la permission, les justifications sont suspectes car ils évoquent principalement : « les autres employés qui sont partis ont gardé l'information » (54%) et « personne ne vérifie ce qui leur appartient » (50%). Seulement 11% ont signalé que leur supérieur leur avait permis de garder l'information. Une des raisons de l'importance de ce phénomène, c'est qu'ils s'opèrent à tous niveaux de l'entreprise et dans tous les départements. Dans cette étude sur 945 employés, tous les départements sont impliqués : 24% des répondants faisaient partie du département des ventes, 20% du département informatique, 16% de l'administration, 10% du département finance et comptabilité, 8% de la communication et marketing et 7% de l'administration générale. Par ailleurs, selon une étude réalisée par les services secrets américains (2008), 62% des employés qui ont volé des données n'ont pas d'antécédents d'arrestations.

Quelles sont les organisations touchées?

Selon l'étude de Verizon (2009), pour tout type de brèches, 31 % sont les commerces de détail et 30% les entreprises de services financiers toutefois ces derniers perdent 93% de toutes les informations compromises. Mais les organisations touchées ne sont pas forcément celles ciblées, car parfois les informations compromises impliquent une tierce partie. D'ailleurs, la détection des brèches est signalée par une tierce partie dans 69% des cas (Verizon, 2009), ce qui indique que les organisations ciblées ont de la difficulté à détecter la perte de leurs données.

Quels sont les documents ciblés?

Les documents qui ont le plus de risque d'être subtilisés selon Ponemon Institute (2009) sont les listes d'adresse de courrier électronique et des dossiers en général. À l'inverse, ce qui intéresse le moins sont les données en format PDF, les bases de données Access et les codes sources. Les moyens utilisés sont aussi variés selon la même étude. 61% des anciens employés ont sous tiré des informations sous la forme papier ou numérique, 53% les ont transférés sur CD/DVD, 42% ont utilisé une clé USB et 38% se sont envoyé les données par mail en fichier joint. On peut cependant soulever que la prépondérance des listes de noms et d'adresses sont les plus ciblés non pas parce qu'elles sont les plus intéressantes, mais parce qu'elles sont les plus faciles à soutirer. D'un autre coté, les secrets commerciaux font l'objet de peu de données et d'études ce qui par conséquent peu induire une réalité cachée. Il est donc important de garder à l'esprit que les conclusions reflètent souvent une partie de la réalité et non pas sa totalité.

Quelles sont les conséquences?

Le coût économique : Tout comme il est difficile d'estimer la proportion du vol et des fuites de données en interne, il est d'autant plus difficile d'en évaluer l'impact. L'estimation du cout engendré par les pertes est large notamment car il n'est généralement pas attribué de valeur économique aux données bien que dans les faits elles en représentent une. Les estimations sont donc généralement des estimations du vol interne comprenant les biens. Selon Wimbush et Dalton (1997), le coût du vol interne serait compris entre 6 milliards et 200 milliards par an et

représenterait 70% des pertes d'une entreprise. Quant au vol de données, Collins (2005) rapporte qu'il serait estimé à 40 milliards de dollars par an. L'estimation, rapportée par Fraumann (1997), évalue le cout annuel de l'espionnage économique dans les sociétés américaines à au moins 50 milliards de dollars. Si on inclut le vol de propriété intellectuelle et les transferts de technologies non restreintes, le cout augmente à 240 milliards de dollars. Cette estimation qui s'approche au mieux de notre sujet d'étude, date tout de même de 1995, on peut donc aisément se dire qu'elles ont augmenté notamment grâce à la diffusion des moyens technologiques. Les organisations canadiennes ont rapporté les cinq conséquences les plus importantes en termes de coût : 1. Répercussion sur la réputation ; 2. Perte de temps due à la perturbation ; 3. Perte de clients ; 4. Actions régulatrices ; 5. Contentieux (Rotman-TELUS, 2009). Le premier élément étant la répercussion sur la réputation, on comprend aisément pourquoi les organisations ne font pas cas des incidents qui se produisent.

Autres conséquences : Les répercussions sur la réputation sont d'autant plus craintes qu'elles sont généralement en lien avec la perte de clients. Les clients qui apprennent que les données les concernant ont fait l'objet d'utilisation frauduleuse sont tentés de rompre ou de ne pas reconduire des contrats ; de modifier leur habitude de consommation pour d'autres magasins… (Collins, 2005). Ce qui a pour effet d'alourdir les pertes financières. Des conséquences à plus long terme peuvent aussi avoir lieu tel que la faillite d'une entreprise notamment en ce qui concerne les entreprises de petites et moyennes taille. La chambre des commerces américaine rapporte que 30% des faillites d'une année données peuvent être attribuables à un problème significatif de vol interne (Hollinger et Clark, 1983). De manière générale, les incidents de ce type affectent les données de l'organisation qui peuvent être modifiées, déplacées…, le réseau et les composants. 96% des incidents affectent l'intégrité, la confidentialité et/ou la disponibilité des données (US secrets services, 2008).

LES FACTEURS « ACTIVATEURS » OU FACTEURS DE RISQUE

Les nouvelles technologies

De manière générale lorsque l'on pense à la fuite de données, on pense immédiatement à internet, probablement parce qu'on la relie à la malveillance externe. Cependant, les supports technologiques eux-mêmes jouent leur rôle dans cette fuite de données or, beaucoup d'organisations continuent d'y accorder peu d'intérêt et donc peu de contrôle. Un tiers des propriétés intellectuelles et des données sensibles des compagnies, allant de numéro de carte de crédit et de sécurité sociale à des informations financières, licences, recherches internes… se trouvent sur des bases de données parfaitement accessibles et sont peu sécurisées (Swartz, 2007). Le matériel d'aujourd'hui aussi maniable que performant facilite le vol, ces outils de travail qui comportent les données, peuvent eux-mêmes être volé avec ce qu'ils contiennent, d'autant plus s'ils sont mal protégés. Ces « hot products » (Felson, 2002) partent donc avec les employés qui quittent l'entreprise. 92% des employés gardent les CD/DVD, 73% les clés USB, 17% les PDA, 9% les Blackberry et 3% les ordinateurs portables (Ponemon, 2009).

Un frein psychologique diminué

Le frein psychologique associé à la déviance, ici au vol de données, est moins opérant que dans d'autres types de délinquance du à l'aspect « immatériel » de l'acte. (Clusif, 2009). Cet aspect immatériel conduit par les technologies a déjà été identifié en 1997 lors d'une enquête réalisée par Kellerhals (in Demeulenaere, 2003) qui montre que lorsque la victime n'est pas clairement identifiée la tendance à défendre ses propres intérêts est plus forte, notamment au détriment d'une entreprise ou d'une institution abstraite.

L'intérêt individuel : Pression économique et déviance comme tricherie

L'action de voler est ici comprise à la fois comme résultant d'éléments personnels et d'éléments sociaux. D'un point de vue sociologique, le vol en interne devrait être moralement proscrit, car se basant sur des règles et des normes partagées de la société. Or on constate que le vol interne en entreprise est bien moins stigmatisé que le vol traditionnel. Demeulenaere (2003) explique cette transgression de la norme par la déviance comme tricherie, c'est-à-dire que l'individu réalise un acte qu'il ne voudrait lui-même pas subir, un peu comme doubler dans une file d'attente. Cette déviance comme tricherie s'explique d'une part par une « *croyance utilitariste qui est que, dans la vie sociale aucune règle n'a de sens et qu'alors chacun doit essayer de faire son intérêt* » et d'autre part car « *le tricheur se croit autorisé moralement à tricher, parce qu'il estime à tort ou à raison, que les autres eux-mêmes trichent tout en prétendant respecter les règles* ». Il y a donc dans les normes « *un décalage entre la visée officielle et la portée effective* » comme l'auteur le souligne.

Pour Hollinger et Clark (1983), le vol interne peut se comprendre comme une « méthode pour acquérir les ressources nécessaires pour résoudre un dilemme financier ». Cette théorie se rapproche de celle de l'anomie de Merton (1938) où face aux buts dominants dans la société, l'individu choisi un moyen déviant pour atteindre ces buts. En lien avec cette idée, la psychologue, E. Dossin, dans le rapport du Clusif (2009) sur la typologie des fraudeurs, détermine le « fraudeur occasionnel et/ou économique par nécessité » pour lequel le besoin va rationaliser son acte. En revanche, cela ne nous explique pas comment et par quel procédé ce qui est volé satisfait les besoins économiques. D'ailleurs, pour Hollinger et Clark (1983) le vol comme manière de répondre à des besoins économique représente une petite proportion.

Settings : Opportunité, attractivité et accessibilité

Ce type de théorie qui prend place dans le cadre de la rationalité du délinquant est à l'heure actuelle une des plus en vogue en gestion de risque et de prévention situationnelle. N'importe qui peut être tenté de voler son employeur si la possibilité lui en est donnée. Cette approche se fonde sur le fait que l'humain est cupide et malhonnête (Hollinger et Clark, 1983) et dépeint une vision fortement pessimiste. Ainsi selon cette théorie, plus il y a d'opportunités, plus il y a de vols. En plus, de l'opportunité, l'attractivité est un point fort des données confidentielles et sensibles. Pour 67% des répondants de l'étude réalisée par Ponemon Institute (2009) sur 945 adultes américains ayant quitté dans les douze derniers mois leur travail, les informations confidentielles et sensibles de leur ancienne compagnie sont utilisées comme un levier pour la recherche d'un nouvel emploi, c'est d'ailleurs la deuxième réponse réponse à la question « pourquoi », les employés disent d'eux même « l'information va me servir pour le futur ». En

plus de leur intérêt majeur dans la suite de leur trajectoire professionnelle, les données visées étaient accessibles puisque tous avaient des ordinateurs et avaient accès à des informations propriétés de l'entreprise comme les données clients, les listes de contacts, données sur les employés, les rapports financiers, documents commerciaux confidentiels, logiciel, licence ou autre propriété intellectuelle. L'étude ne dit pas en revanche si les sujets avaient besoin de l'ensemble des données dont ils avaient l'accès pour exercer leur fonction. De plus, l'accessibilité des données est généralement conservée même après le départ de l'employé. 24% des répondants avaient encore accès après leur départ aux données de l'entreprise. 38% des répondants ont su que leur accès était encore possible par leurs collègues. 51% disent que leur supérieur leur a dit, 44% continuent de recevoir des courriers électroniques du compte de leur compagnie et 4% utilisent l'accès de leurs anciens collègues.

La frustration : insatisfaction, sentiment d'injustice et vengeance

Hollinger et Clark (1983) reconnaissent en l'insatisfaction un facteur important dans l'augmentation du vol interne. Selon eux, si les employés se sentent exploités par l'entreprise ou par leur supérieur, c'est-à-dire ceux qui représentent la compagnie, les employés seront plus impliqués dans des comportements allant à l'encontre de l'organisation. Dix ans plus tard, Murphy (1993) établit le même constat selon lequel les individus satisfaits adoptent des comportements prosociaux alors que ceux qui ne le sont pas ont tendance à s'engager dans des actes de déviance contre l'organisation. Pour Greenberg (1997), le vol peut être compris comme une manière de rétablir un équilibre entre les parties. Cette théorie s'inscrit dans la lignée de la théorie de l'équité d'Adams selon laquelle les employés qui jugent ne pas être suffisamment payés augmentent ce salaire par le vol. Cependant, plus que le montant du salaire en lui-même c'est la façon d'être considéré qui importe. Dans l'expérience menée par Greenberg (1997), le groupe qui subit une réduction de salaire sans informations est plus impliqué dans le vol que dans le groupe où cette même réduction de salaire est complétée par un traitement social plus sensible. Si les employés ne se sentent pas reconnus pour leur travail, cela amène parfois à un sentiment de vengeance. Dans l'étude du Clusif (2009) E. Dossin, psychologue, distingue 4 types de fraudeurs dont le premier, le vengeur a pour unique motivation la vengeance, il est donc inoffensif tant qu'il ne se sent pas menacé. Mais si la pression augmente, son hypersensibilité narcissique sera touchée et il passera à l'acte avec l'objectif d'atteindre son employeur. La relation entre employé et employeur est donc importante en tant que facteur de risque. Une autre étude allant dans ce sens est celle des services secrets américains (2008) selon laquelle dans 73% des cas, il existe une série d'événements qui déclenche les actions internes et pour 67% il s'agit d'événements reliés au travail comme un licenciement (37%) ou une dispute avec l'employeur (20%). Les employés questionnés par l'étude Ponemon (2009) donnent en 5^{e} position « la compagnie de mérite pas de garder cette information » qui confirme le sentiment d'insatisfaction. Par ailleurs, selon cette même étude, 66% des individus ayant une opinion négative de leur employeur sont partis avec les données de l'entreprise alors que seulement 26% de ceux qui avaient une opinion positive sont partis avec les données.

Le vol intégré comme norme

Lorsqu'on demande aux anciens employés d'une société pourquoi ils ont pris des informations de l'entreprise en quittant leur emploi tout en sachant que ça ne leur était pas autorisé, la première réponse qui est donnée est : « Tout le monde le fait » (Ponemon, 2009). Le groupe de

travail n'échappe pas à la création de normes informelles internes. Le vol en interne notamment, persiste car la norme informelle le permet dans une certaine mesure même si la norme formelle (celle du contrat) l'interdit. D'ailleurs, ce sont les sanctions informelles qui déterminent le mieux les limites tolérables des comportements déviants sur le lieu de travail (Hollinger et Clark, 1983). Les contrôles formels à l'inverse peuvent influencer de manière négative le phénomène du vol interne alors que les contrôles informels réalisés par les groupes sont les plus efficaces. Le vol interne devient une règle implicite qui supplante la règle officielle et qui peut même faire l'objet d'un échange entre salariés et managers[1]. Ainsi comme le souligne Greenberg (1997) l'organisation encourage, ou du moins tolère le vol dans le cadre d'un seuil à respecter. Le vol peut donc revêtir des utilités : pour les supérieurs, c'est une façon de contrôler les employés par l'utilisation de ce « salaire invisible » mais aussi pour les employés eux-mêmes puisqu'il peut s'agir de comportements prosociaux envers le groupe dont la norme de vol est admise. Ce dernier est qualifié de « support motive » selon Greenberg (1997).

La participation active à la création de ces données

Si l'on peut donner une meilleure justification au vol de donnée, ça serait celle-ci : « j'ai participé à la création de cette information » (Ponemon, 2009). Bien que les données soient considérées comme la propriété de l'entreprise, on comprend ici que l'employé qui a participé à l'élaboration d'un projet puisse percevoir ces informations comme lui appartenant. Il ne va donc pas considérer cela comme du vol puisqu'issu en partie de son travail personnel.

L'impunité

Si le vol est aussi courant dans certaines organisations, c'est que d'une part il fait partie d'une certaine norme, comme nous l'avons évoqué plus haut, mais aussi parce que les individus jouissent d'une certaine sécurité. Les risques encourus sont minimes par rapport aux bénéfices. L'employé malveillant risque au pire d'être renvoyé, ce qui est assez rare car le renvoi d'un salarié est aussi couteux pour la société, elle ne prendra cette mesure que si le vol atteint une forte valeur en une seule fois ou qu'elle met à l'épreuve sa compétitivité. L'employé ne risque pas d'être poursuivi car les organisations préfèrent gérer en interne afin de réduire l'impact médiatique que l'événement pourrait avoir sur elles. Encore faut-il que l'organisation le découvre, car pour bon nombre d'employés : « l'entreprise ne peut pas me retracer » et profite ainsi d'un sentiment d'impunité, confirmé par une certaine norme établie.

Climat de travail et éthique

Comme nous avons pu le constater précédemment, la relation entre employés et employeur peut être un élément facilitateur du vol en interne. Plus largement, le climat de travail peut jouer un rôle. L'étude de Weber (2003) montre une différence significative entre deux organisations selon les climats éthiques de travail (« ethical work climates, EWCs). Selon les résultats, l'organisation qui possède un climat éthique de travail favorisant la morale n'est pas sujette au vol interne. Cependant, on peut douter des résultats tranchés de l'étude, car il est impossible à notre idée d'obtenir un taux de vol égal à zéro.

[1] Voir un précédent travail : Le vol en interne : absence de contrôle social ?

MESURES PRÉVENTIVES

Nous avons pu constater qu'il existe de nombreux facteurs qui peuvent intervenir dans la régulation du vol en interne. Cependant, nous avons aussi constaté que le vol de données est foncièrement négligé par les entreprises. En effet, rappelons que seulement 15% des entreprises réalisent des analyses sur ce phénomène. De plus, parmi celles-ci 45% sont jugées incomplètes et 29% jugées superficielles (Ponemon, 2009). Dans cette section, nous proposons quelques avenues possibles pour limiter les risques de pertes de données aussi bien malveillantes qu'accidentelles.

Bases de données

La difficulté du contrôle des données réside dans le fait qu'elles sont dynamiques, elles sont continuellement en évolutions, supprimées, ajoutées, modifiées… Afin de les protéger, il faut donc que le contrôle soit aussi dynamique, les politiques de protection doivent donc suivre des mises à jour régulières (Swartz, 2007).

Limiter les accès

Dans la majorité des cas, les salariés ont accès aux informations qu'ils peuvent soustraire sur le lieu de travail ou en dehors et cela même après qu'un individu ait quitté l'entreprise (US Secret Services, 2008). Les politiques de sécurité doivent donc comprendre la limitation des accès en sélectionnant qui a accès à quoi selon les besoins des différents postes et les protéger par des mots de passe.

Le contrôle des supports

Les ordinateurs portables, les cellulaires, clés USB, PDA, iPod… rendent la tâche facile pour des employés désireux de retirer des données de l'organisation, les compagnies doivent pouvoir contrôler quelles informations peuvent être téléchargé, copié dans ces appareils et ceux qui ne le doivent pas (Swartz, 2007).

Mesurer le risque

Bien qu'il soit difficile d'attribuer une valeur aux propriétés intellectuelles d'une organisation étant donnée sa disponibilité, sa confidentialité, les impacts doivent être quantifiables. Pour cela, il faut analyser les frais engagés pour la réparation et le maintien de l'activité économique de l'organisation ainsi que les pertes potentielles en termes de chiffres d'affaires, de clients… (Clusif, 2009). Il est aussi important d'obtenir une meilleure transparence du phénomène dans sa propre organisation car bon nombre d'entreprises admettent qu'elles ne détectent qu'une petite minorité des vols (Hollinger & Clark, 1983). Cette transparence passe aussi par la délimitation de ce qui est toléré et de ce qui ne l'est pas. Sachant qu'une entreprise ne peut espérer éliminer totalement la perte de donnée, notamment car la négligence est toujours possible, il peut être admis un taux de vol acceptable qui ne portera pas préjudice à l'organisation. Le climat de travail peut être modifié afin de transformer les perceptions des employés (Kulas, 2007).

Conscientiser

S'il est admis que voler est moralement incorrect, il est important de rappeler à travers des éléments simples les termes de certains contrats de travail. L'étude réalisée par les services secrets américains (2008) montre que seulement dans la moitié des cas de vol de propriété intellectuelle, les employés ont eu à signer un accord de non-divulgation ou étaient au courant des politiques concernant la confidentialité. Nous avons aussi pu constater plus haut que le fait de participer à certains projets rendent floues les limites entre la propriété de l'entreprise et celle de l'individu. Il est donc important dans un premier temps de rappeler les termes de confidentialité qui s'appliquent. Par ailleurs, dans un second temps, nous avons remarqué que le frein psychologique associé au vol est diminué du fait de l'absence de « personnalisation». Il est donc tout aussi utile dans un deuxième temps de permettre cette personnalisation en sensibilisant sur les conséquences à court terme et à long terme de la perte d'informations. Comme le souligne Greenberg (1997), le vol s'institutionnalise comme norme car les personnes qui sont impliquées pensent en retirer que des bénéfices et aucun inconvénient. En donnant des feedbacks explicites sur ce type de comportement, il y a de fortes chances que les individus perçoivent mieux les impacts. D'autant que cette mesure est tout aussi utile contre la malveillance interne ainsi que la négligence.

Instaurer un climat positif, traiter les employés avec respect

Si cela peut paraître évident, nous avons rappelé comment la frustration pouvait être à l'origine de comportement déviant dans les organisations. Il est donc important de minimiser cette frustration en traitant les personnes avec respect car « il est plus difficile de voler un ami qu'une personne qui ne se préoccupe pas de vous» (Greenberg, 1997 ; Everton et coll., 2005).

CONCLUSION

La fuite de données en interne est un domaine vaste et varié, ces fuites peuvent prendre des formes très différentes à travers la négligence, le vol ou l'espionnage. On peut noter toutefois qu'il s'agit d'un phénomène très répandu et peu étudié empiriquement ce qui l'entoure d'un chiffre noir relativement important. Au niveau du vol d'information, il n'existe pas de théories centrées sur ce problème mais généralement portées sur les comportements antisociaux contre l'entreprise ou sur le vol de manière large. À travers la littérature, nous avons tenté de repérer les facteurs de risque qui pouvaient être à l'origine du passage à l'acte. Nous pouvons raisonnablement penser qu'un seul facteur ne suffit pas, mais que la combinaison de plusieurs est plus pertinente. Ce travail aura permis d'élargir davantage les connaissances à propos de ce problème reconnu comme tel par les organisations. Il est cependant indéniable que de futures recherches creusent davantage la compréhension de celui-ci car l'information constitue aujourd'hui une composante clé de la compétitivité des entreprises, c'est un actif stratégique (Barel, 2009). Quant à la prévention qui peut être faite, le constat réalisé pour les facteurs de risque s'applique aux mesures : la combinaison de plusieurs mesures tant managériales que techniques, répondra mieux aux problématiques particulières à chaque organisation. Il est donc là aussi nécessaire d'obtenir plus de données pour pouvoir répondre de manière adéquate. Enfin, il est important de noter que la responsabilité des pertes n'incombe pas uniquement à une seule personne puisqu'entre en jeu des facteurs à la fois individuels, sociaux, économiques… dont il faut tenir compte.

Références

Barel, M. (2009).Le vol d'informations n'existe pas. . . Quelles voies juridiques pour la protection de l'information ? *Actes du 7e symposium sur la sécurité des technologies de l'information et des communications* (SSTIC), p. 193-200

Bonnet, F. (2008). Un crime sans déviance : le vol en interne comme activité routinière. Revue française de sociologie, vol. 49 (2), p.331-350

Bonnet, F. (2007). Le vol en interne : les vols commis par les salariés sur leur lieu de travail (= Employee theft : a littérature review). Sociologie du travail, vol.49 (4), p.544-556.

Caprioli, A.(2008). Le « recel »d'informations et des correspondances sanctionné. *Revue Communication - Commerce Electronique*, no 3, comm. 46 (6).

Clusif (2009). Fraude interne, malveillance interne : détection et gestion. *Les synthèses du Clusif*, Synthèse de la conférence thématique du CLUSIF du 4 juin 2009 à Paris.

Collins, J. (2005). Preventing Identity Theft in Your Business: How to Protect Your Business, Customers, and Employees , Hoboken, NJ, John Wiley and Sons, Inc., 245p.

Cyber-Ark (2008). The global recession and its effect on works ethics. *Cyber-Ark Software Survey*, Decembre 2008.

De Dreu, C.K.W. (2006) Rational Self-Interest and Other Orientation in Organizational Behavior: A Critical Appraisal and Extension of Meglino and Korsgaard. *Journal of Applied Psychology*, Vol.91, p.1245-1252.

Demeulenaere, (2003). Les normes sociales. Entre accords et désaccords, Paris, P.U.F., collection "Sociologies".

Dupré, J. (2001). Espionnage économique et droit: l'inutile création d'un bien informationnel. *Lex Electronica*, vol. 7(1), http://www.lex-electronica.org/articles/v7-1/Dupre.htm

Everton, W.; Jolton, J. & Mastrangelo, P. (2007). Be nice and fair or else: understanding reasons for employees' deviant behaviors. *Journal of Management Development*, Vol. 26 (2), p.117-131

Felson, M. (2002). *Crime and everyday life*. Thousand Oaks, Cal : Pine Forge, 3 rd édition

Fraumann, E.(1997). Economic espionage: security missions redefined. *Public Administration Review*, Vol. 57(4), p.303

Gallet, O. (2005). Halte aux fraude$: Prévenir et détecter les fraudes en entreprise. Paris : Dunod

Greenberg, J. (1997). The Steal Motive: Managing the social determinants of employee theft. In R. Giacalone & J. Greenberg (Eds.), Antisocial behavior in organizations (p. 85-108). Thousand Oaks, CA: Sage.

Greenberg, J. (2002).Who stole the money, and when? Individual and situational determinants of employee theft. *Organizational Behavior and Human Decision Processes*, Vol. 89, p.985–1003.

Hancock, B. (1999). Security views. *Computers & Security*, Vol.18, p.184-198

Heffernan, R. ; Moberly, M. ; Peterson, K. & Runyon, L. (2007). Trends in Proprietary Information Loss. *Survey Report*. Asis International, aout 2007. 52p.

Hejazi,W. & Lefort, A. (2009). Rotman-TELUS Joint Study on Canadian IT Security Practices. rotman.utoronto.ca/securitystudy.

Hollinger, R. C., & Clark, J. P. (1983). Theft by employees. Lexington, MA: Lexington Books.

Jones, J.W., Slora, K.B. & Boye, M.W. (1990), Theft reduction through personnel selection: a control group design in the supermarket industry. *Journal of Business and Psychology*, Vol. 5 p.275-279.

Kowalski, E. ; Cappelli, D. & Moore, A. (2008). Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector. United States Secret Service.

Kulas, J. T., Roberts, J. E., DeMuth, R. L. F., & Jadwinski, V. (2007). Employee satisfaction and theft: Testing climate perceptions as a mediator. *Journal of Psychology: Interdisciplinary and Applied,* Vol.141*,* 389-402*.*

Mars, G. (1983). Cheats at Work. An Anthropology of Workplace Crime. London, George Allen & Unwin.

Merriam, D. (1977). Employee theft, *Criminal Justice Abstracts* **nº 9,** pp. 380–386.
Merton, R.K (1938). Social Structure and Anomie. *American Sociological Review* 3, p. 672-82.

Ogren, E. (2007). Intellectual property rules, *Information Security Brief*. Entreprise Strategy Group.

Payne, R. (1971). Les Espions Dans l'Usine. Paris, Fayard, 233 p.

Ponemon Institute (2009). Data Loss Risks During Downsizing : As Employees Exit, so does Corporate Data. White-paper, février 2009

Spector, P. E. (1997). The role of frustration in antisocial behavior at work. In R. A. Giacalone & J. Greenberg (Eds.), *Anti-social behavior in organizations* (p. 1–17). Thousand Oaks: Sage.

Swartz, N. (2007). Protecting information from insiders. *Information Management Journal*, Vol. *41*(3), p.20-24.

Verizon Business Risk Team (2009). Data Breach Investigations Report.

Weber, J. ; Kurke, L. & Pentico, D. (2003). Why do employee steal? Assessing Differences in Ethical and Unethical Employee Behavior Using Ethical Work Climates. Business & Society, Vol. 42 (3), p. 359-380.

Wimbush J.C. & Dalton. D. R*.(1997). Base rate* for employee theft: convergence of multiple methods. *Journal of Applied Psychology*, Vol. 82. (5), p.756-763