Dossier

L'entreprise face aux fuites de données

Le vol interne d'informations : modéliser et mesurer les facteurs de risque

Les affaires Wikileaks et Renault l'ont illustré à merveille : une entreprise ou un Etat peut dresser une forteresse pour se protéger contre l'extérieur, celle-ci ne la protégera en rien des menaces qui émanent de l'intérieur. La problématique du vol interne s'est imposée au sommet des priorités de ces acteurs, et quelques études de sondage ont accrédité l'ampleur du phénomène. Toutefois, ainsi que le rappellent Audrey Asseman et Benoit Dupont, aucune étude empirique ne se concentre sur les facteurs explicatifs du vol interne. Carence désormais comblée avec l'enquête réalisée par ces deux auteurs, dont les résultats évoqués exclusivement dans cet article permettent de mesurer l'importance respective de ces facteurs dans la dynamique du vol d'informations sensibles. Des données indispensables pour formuler une politique de prévention efficace en la matière. Les auteurs comparent alors ces résultats avec les mêmes facteurs tels qu'ils sont recensés par la littérature académique (facteurs situationnels, psychologiques, sociaux et psychosociaux).

La divulgation en 2010 de plus de 700 000 documents confidentiels provenant du Pentagone (les *War Logs* des guerres d'Irak et d'Afghanistan) et du Département d'État par le site Wikileaks a causé un embarras diplomatique d'une ampleur inégalée pour la diplomatie américaine. Elle a par ailleurs donné lieu à des rebondissements informatiques et judiciaires qui ont entraîné un déluge de commentaires et d'analyses plus ou moins pertinents sur la fin du secret (et par extension du mensonge) comme paramètre de l'action gouvernementale, sur le déclenchement de la première « cyberguerre », ou encore sur l'émergence hypothétique d'un nouveau modèle de journalisme. Derrière les hyperboles médiatiques et un parfum d'intrigue évocateur des romans d'espionnage, se trouve pourtant un évènement déclencheur d'une grande banalité : un jeune soldat désabusé et mentalement fragilisé par une rupture amoureuse est envoyé en Irak dans le cadre de ses fonctions d'analyste de renseignement. Peut-être poussé à bout par la torpeur de l'été bagdadien ou par l'écoute répétée du dernier album de Lady Gaga, il décide alors de télécharger des quantités massives d'informations sensibles sur un CD-Rom portant le nom de cette artiste et de le communiquer à Julian Assange, le responsable de Wikileaks. L'enquête

menée par l'armée américaine démontra que les locaux dans lesquels il travaillait ne respectaient pas les normes de sécurité exigées au regard de la confidentialité des informations traitées (Jaffe et Nakashima, 2011). Pourtant, on aurait tort de voir là la convergence d'un ensemble de circonstances exceptionnelles. En effet, ces données sont accessibles à plus de 500 000 militaires, diplomates et policiers via le réseau Siprnet (*Secret Internet Protocol Router Network*), qui est administré par le ministère américain de la défense. Dès 2008, les risques de fuites d'informations découlant de négligences ou de malveillances dans la gestion d'un système aussi complexe avaient été évoqués dans un rapport remis au Pentagone, mais sans qu'aucune des recommandations formulées ne soit mise en œuvre (Nakashima, 2010).

Le Pentagone n'est pas la seule organisation confrontée à ce type de problème. La protection des données et des informations confidentielles représente un défi de taille pour l'ensemble des organisations publiques et privées dans un contexte où les affaires de pertes ou de vols de données se multiplient.

La fuite d'informations en interne est d'autant plus préjudiciable que la sévérité du risque est plus élevée que pour les menaces externes.

Ainsi, une étude menée en 2009 auprès de 300 professionnels de la sécurité et des technologies de l'information au Canada (Hejazi et Lefort, 2009) indiquait une augmentation de 112 % des incidents liés à l'accès non autorisé à des informations par des employés au cours de l'année précédente. Par ailleurs, le vol d'informations appartenant aux organisations sondées a augmenté de 75 % pendant la même période. Un autre sondage mené par CyberArk (2008) auprès de 600 répondants anglais, hollandais et américains sur le vol d'informations en interne a démontré que 25 % des employés anglais, 52 % des employés américains et 31 % des employés hollandais partiraient avec des informations s'ils en avaient l'occasion. La fuite d'informations en interne est d'autant plus préjudiciable que la sévérité du risque est plus élevée que pour les menaces externes. En raison de leur accès privilégié, les employés peuvent identifier et prélever les informations les plus sensibles de l'organisation, ce qui exige des efforts beaucoup plus importants de la part des pirates informatiques. Une étude réalisée par Verizon (2009) montre que 20 % des incidents de vols d'informations sont causés par les employés de l'entreprise victime, et que deux tiers de ces incidents sont d'origine malveillante. Quant au Clusif (2009), il estime que 80 % de la malveillance proviendrait de l'intérieur de l'organisation.

61 % des répondants estiment que les données sont facilement accessibles à l'ensemble des employés.

Les préjudices subis par les entreprises victimes incluent évidemment le coût économique direct, mais les pertes de données et d'informations confidentielles entraînent également des répercussions négatives sur la réputation de l'organisation, un gaspillage de ressources affectées au rétablissement des systèmes et à la reconstitution des données, la perte de clients et de fournisseurs, ainsi que l'imposition d'amendes par les autorités réglementaires (Hejazi et Lefort, 2009). Dans un tel contexte, il nous est paru utile de comprendre quels sont les divers facteurs de risque associés au vol de données et d'informations en interne tels qu'ils apparaissent dans la littérature scientifique. Dans la seconde partie de cet article, nous présentons les résultats préliminaires d'un sondage mené auprès de 66 répondants et qui

avait pour objet de mesurer l'importance respective de ces facteurs dans la dynamique du vol d'informations sensibles. Cette enquête a en effet confirmé le manque de protection des informations détenues par les entreprises, puisqu'environ 61 % des répondants estiment que les données sont facilement accessibles à l'ensemble des employés. Appuyant cette idée, environ 60 % des individus considèrent que les outils mis à leur disposition ne sont pas convenablement sécurisés.

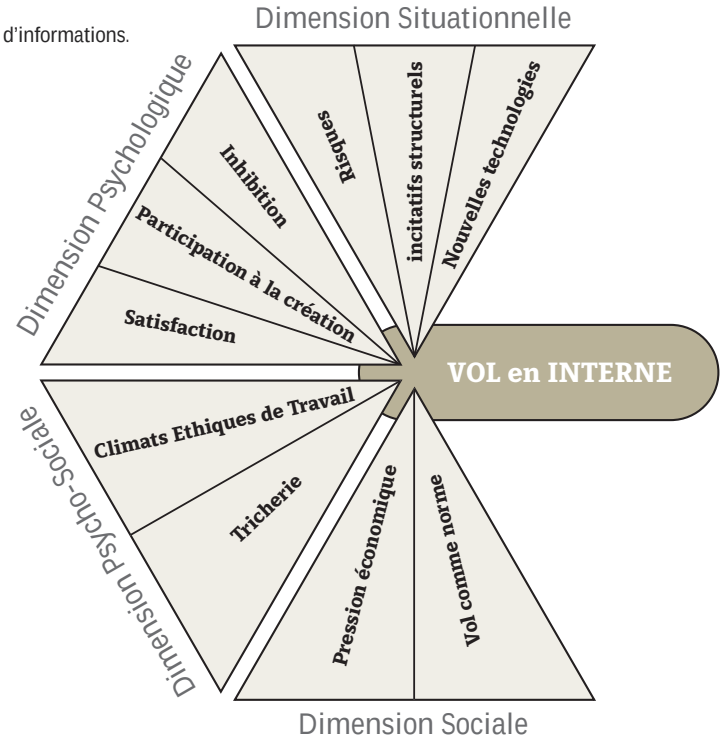
Les facteurs de risque du vol d'informations en interne : modéliser la déviance organisationnelle

Étant donné le peu de travaux consacrés au vol de données et d'informations en interne, nous avons eu recours à des études sur des phénomènes connexes réalisées dans les trois disciplines suivantes : criminologie, sociologie du travail et psychologie. La recension de cette littérature nous a permis d'identifier un certain nombre de facteurs facilitant le vol d'informations et de données en interne. Ces dix facteurs peuvent être regroupés en quatre dimensions que le schéma ci-dessous nous aide à visualiser.

Dimension situationnelle

La dimension situationnelle regroupe les facteurs liés à l'environnement de travail. Premièrement, nous supposons que l'utilisation des nouvelles technologies par les entreprises présente un risque accru en matière de vol d'informations et de données en interne. La variété des supports de stockage et des canaux d'échange, ainsi que la numérisation systématique des données de l'entreprise créent un environnement au sein duquel l'information circule de manière très fluide, par

Schéma 1 :
Les 10 facteurs de risque du vol d'informations.



contraste avec un contexte traditionnel où le règne du papier oppose des contraintes physiques importantes au vol massif de données. Les 250.000 câbles diplomatiques transmis à Wikileaks ont ainsi pu être gravés sur un seul CD-Rom, alors que les 260 millions de mots qu'ils contiennent auraient nécessité plus de 577.000 feuilles de papier s'ils avaient dû être imprimés au format Word. Ces équipements portables sont ainsi des « *hot products* » (Felson, 2002) que les employés qui quittent l'entreprise n'hésitent pas à s'approprier. On note qu'à leur départ (volontaire ou forcé), 92 % des employés conservent des CD/DVD-Rom obtenus dans le cadre de leurs fonctions professionnelles, et les chiffres pour les clés USB (73 %) et les téléphones intelligents et les agendas électroniques (26%) sont étonnamment élevés (Ponemon, 2009).

Plus le nombre d'opportunités serait élevé, plus on observerait de vols de données et d'informations.

Le facteur des « incitatifs structurels » fait référence à la théorie de la prévention situationnelle. Ce facteur comporte des éléments d'opportunité qui se traduisent selon Felson (2002) par une absence de gardiens qui dissuaderaient l'individu rationnel de passer à l'acte. Ainsi, plus le nombre d'opportunités serait élevé, plus on observerait de vols de données et d'informations. Les éléments d'attractivité font eux référence à la cible visée : les informations et données obtenues frauduleusement doivent être utiles ou profitables pour l'individu. Les documents confidentiels et sensibles représentent en substance une forte attractivité dans un environnement économique extrêmement compétitif. Une étude réalisée par Ponemon (2009) montre par exemple que 67 % des employés ayant quitté leur emploi au cours des douze derniers mois considèrent que les informations confidentielles et sensibles de leur ancienne entreprise constituent un levier dans la recherche d'un nouvel emploi.

L'accessibilité excessive à la propriété intellectuelle de l'entreprise se prolonge souvent après le départ d'un employé.

Le dernier élément est celui de l'accessibilité, c'est-à-dire de la facilité à soustraire les informations convoitées à la vigilance de l'organisation. Cette accessibilité prend la forme d'accès non restreints aux bases de données ou à toute propriété intellectuelle de l'entreprise. De plus, on constate que l'accessibilité excessive se prolonge souvent après le départ d'un employé. En effet, 24 % des répondants à l'étude Ponemon (2009) affirment avoir eu accès aux données de l'entreprise après leur départ, 38 % par le biais d'anciens collègues, 51 % par l'intermédiaire de leur supérieur, alors que 44 % continuent de recevoir des courriers électroniques du compte de leur compagnie.

Enfin, le facteur « risques » s'inscrit toujours dans la perspective de l'analyse coûts-bénéfices. Alors que la cible visée représente un bénéfice important, le risque, donc le coût, est souvent négligeable. En effet, l'employé malveillant risque tout au plus d'être congédié dans les situations où la valeur de l'information dérobée dépasse le coût induit par le renvoi ou qu'elle met en jeu la compétitivité de l'organisation. De plus, la résolution de ce type de problème est exclusivement gérée par les instances internes, afin de réduire l'impact médiatique sur l'image de l'organisation. Peu d'incidents font donc l'objet de poursuites, ce qui érode le pouvoir dissuasif des institutions pénales. En dernier lieu, la plupart des vols de données et d'informations en interne ne sont pas détectés par les organisations qui en sont les victimes, ce qui contribue à renforcer le sentiment d'impunité des délinquants.

Dimension sociale

La crise financière que nous traversons et les modes de vie contemporains d'hyper-consommation pourraient aussi expliquer en partie ce type de comportements. Le facteur « pression économique » traduit l'hypothèse soulevée par Hollinger et Clark (1983) que le vol interne peut se comprendre comme une « *méthode d'acquisition des ressources nécessaires pour résoudre un dilemme financier* ». Cette théorie d'inspiration Mertonienne voit dans le passage à l'acte le résultat d'un processus d'adaptation à une situation de frustration financière. Confirmant cette idée, la psychologue Estelle Dossin identifie « *le fraudeur occasionnel par nécessité* » dans la typologie des fraudeurs présentée au Clusif (2009). Pour ce type de fraudeur, le besoin va venir rationaliser l'acte. Ainsi, contrairement à une logique du vol d'informations comme stratégie de promotion à l'externe, le bénéfice serait ici uniquement d'ordre pécuniaire dans une logique de revente à des compétiteurs généreux.

> **Le vol interne peut se comprendre comme une « *méthode d'acquisition des ressources nécessaires pour résoudre un dilemme financier* ».**

Par ailleurs, notre société énonce à travers des normes et des règles partagées ce qu'il est permis ou non de faire. Le vol étant moralement proscrit, il serait donc logique que le vol d'informations et de données en interne le soit aussi. Pourtant, on remarque que ce dernier est bien moins stigmatisé que le vol traditionnel. Le facteur « vol comme norme » explique pourquoi certains actes d'ordinaire considérés déviants ne se verront pas apposés d'une telle étiquette. C'est généralement le cas des délits commis en entreprise. En effet, dans le milieu de travail, les normes informelles régissant les relations entre collègues peuvent se substituer aux normes formelles formulées par le contrat de travail par exemple. Les normes informelles issues des pratiques quotidiennes ont plus de poids que les normes formelles, car elles sont associées à des sanctions informelles qui déterminent de manière beaucoup plus contraignante les limites tolérables des comportements déviants sur le lieu de travail (Hollinger et Clark, 1983). Ainsi, dans notre cas, lorsqu'on demande à d'anciens employés ayant quitté leur emploi pourquoi ils ont pris avec eux des informations appartenant à l'entreprise tout en sachant que cela était illégal, la réponse la plus fréquente est : « parce que tout le monde le fait » (Ponemon, 2009). On constate alors que le vol d'informations n'est pas considéré comme déviant, mais au contraire intégré comme norme.

> **Le vol d'informations n'est pas considéré comme déviant, mais au contraire intégré comme norme.**

Dimension psychologique

Le premier facteur de la dimension psychologique est celui de « l'inhibition ». La plupart d'entre nous disposent d'une inhibition psychologique associée à la déviance. Nous envisageons les conséquences de nos actes sur nous-mêmes et sur autrui et de manière générale, nous éprouvons une certaine empathie envers les victimes potentielles, nous dissuadant alors d'agir de manière répréhensible. Dans le cas du vol de données et d'informations, cette inhibition psychologique est moins opérante que pour d'autres types de délinquance en raison de l'aspect « immatériel » de l'acte (Clusif, 2009). Cet aspect immatériel renforcé par les technologies a 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 la plus forte, notamment au détriment d'une entreprise ou d'une institution abstraite.

Les individus qui ont travaillé ou participé à un projet perçoivent les informations qui en découlent comme leur appartenant.

Une autre justification fréquemment utilisée dans les cas de vols de données et d'informations est celle de la « *participation à la création* » (Ponemon, 2009). En effet, bien que tout ce qui est conçu dans une entreprise, y compris de nouveaux procédés, constitue la propriété de celle-ci (dans ce cas, la propriété intellectuelle), les individus qui ont travaillé ou participé à un projet perçoivent les informations qui en découlent comme leur appartenant. Ils estiment qu'il s'agit du fruit de leur réflexion et que le fait de partir avec ce type d'informations ne peut pas être considéré comme un vol.

Enfin, un des traits les plus souvent abordés en contexte de travail vis-à-vis des comportements dits « *antisociaux* » est celui de la satisfaction. Le facteur « *satisfaction* », ou plutôt l'absence de satisfaction au travail, est reconnu par Hollinger et Clark (1983) comme un déterminant important de l'augmentation du vol en interne. Selon ces deux auteurs, si les employés se sentent exploités par l'entreprise ou par leur supérieur, ils verront moins d'objections à adopter des comportements allant à l'encontre des intérêts de l'organisation. Dix ans plus tard, Murphy (1993) dresse un constat similaire selon lequel les individus insatisfaits 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 l'équilibre entre les parties. Cette théorie s'inscrit dans la lignée de la théorie de l'équité d'Adams (1965) selon laquelle les employés qui jugent être insuffisamment payés complètent leur salaire par le vol. Cependant, plus que le montant du salaire en lui-même, c'est la façon d'être considéré qui importe. Si les employés ne se sentent pas reconnus pour leur travail, ils peuvent être amenés à développer un sentiment de vengeance. Parmi les quatre types de fraudeurs identifiés par Estelle Dossin, le « *vengeur* » est qualifié d'inoffensif tant qu'il ne se sent pas menacé (Clusif, 2009). Toutefois, si la pression augmente, son hypersensibilité narcissique sera affectée et il passera à l'acte avec l'objectif d'atteindre son employeur. La relation entre employé et employeur est donc un facteur de risque important. Confirmant cette idée, une étude des Services Secrets américains (Kowalski, Cappelli et Moore, 2008) montre que dans 73 % des cas, les vols internes sont précédés d'événements reliés aux conditions de travail tels qu'un licenciement (37 %) ou un litige avec l'employeur (20 %).

Les individus insatisfaits ont tendance à s'engager dans des actes de déviance contre l'organisation.

Dimension psychosociale

Ce groupe de facteurs occupe un espace intermédiaire entre la dimension sociale des interactions qui se focalise sur les liens entre employés, et la dimension psychologique qui recouvre les interprétations individuelles faites par chaque membre de l'organisation de sa place au sein de cette dernière. Le facteur « CETs » est l'acronyme de « Climats éthiques de travail ». Cette notion fait référence à l'existence (ou pas) de politiques en matière de comportements éthiques sur le lieu de travail et à leur influence sur les comportements des employés. Selon une étude de Weber (2003), les organisations qui suscitent un climat de travail fortement ancré dans des valeurs morales

sont beaucoup moins exposées au vol interne que celles où le climat de travail élude cette démarche éthique.

Le facteur « tricherie » explique le vol comme un acte que l'auteur juge répréhensible mais que d'autres n'hésitent pas à commettre, ce qui le décharge à ses yeux de tout sentiment de culpabilité. Ce modèle utilitariste repose sur la « *croyance [...] que, dans la vie sociale aucune règle n'a de sens et qu'alors chacun doit essayer de faire selon son intérêt* », et que « *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* » (Demeulenaere, 2003). Le décalage entre la formulation officielle des normes et les pratiques de contournement observées sert donc de levier à l'individu pour justifier des actes qu'il sait être pertinemment illégaux.

Mesurer les facteurs de risque : les enseignements d'une étude exploratoire

Les divers facteurs de risque recensés dans la littérature proviennent d'études basées sur des cadres théoriques et des méthodologies de recherche très diversifiés, ce qui ne nous permet pas de savoir comment ils interagissent les uns avec les autres, ni lesquels de ces facteurs sont les plus influents sur le vol de données et d'informations. Nous avons donc élaboré un instrument de mesure capable de prendre en compte l'ensemble de ces facteurs, et nous l'avons administré sous forme de sondage. L'objectif était de déterminer quels facteurs doivent être prioritaires en termes de prévention afin de réduire les risques de vols d'informations en interne.

Méthodologie

Nous avons créé un questionnaire comportant plusieurs questions pour chacun des facteurs de risque identifiés. Pour certains d'entre eux, tels que la satisfaction ou le climat de travail, nous nous sommes inspirés d'échelles qui existaient déjà et nous les avons adaptées au vol d'informations et de données. Pour d'autres, nous avons imaginé des scénarios qui pouvaient avoir lieu en situation de travail afin d'observer la fréquence de ces comportements ainsi que l'opinion des individus par rapport à ceux-ci. L'échantillonnage dit par « boule de neige » a permis de récolter 66 réponses. Malgré une large diffusion et de nombreux efforts auprès de grandes organisations canadiennes et françaises touchées par ce phénomène, nous constatons un taux de réponse assez faible, ce qui laisse entendre que la fuite de données est un sujet encore tabou et difficile à évaluer. Notre échantillon est majoritairement masculin (69,7 % des répondants), et est constitué de 45,5 % de cadres. Le département le plus représenté est celui de la Direction et de la stratégie (25,8 %), suivi des Ressources humaines et de la Production et Ingénierie (12,1 % chacun). Ces trois grandes fonctions semblent les plus particulièrement concernées par la fuite d'informations et semblent assez enclines à chercher des solutions afin de répondre à ce type de problème.
À l'inverse, nous nous étonnons de la sous-représentation des fonctions de Recherche et Développement (4,5%) et de Gestion financière (1,5%), alors que les informations dont elles disposent sont également stratégiques pour l'organisation. Le questionnaire qui demandait aux répondants d'évaluer la prévalence des vols d'informations au sein de leur organisation a été transmis de manière électronique. Les réponses étaient anonymes et confidentielles.

Résultats

Bien que des analyses statistiques bivariées et multivariées aient été menées afin de comprendre les interactions entre les différents facteurs et la perception des répondants, nous présentons ici les statistiques descriptives les plus significatives pour les éléments du modèle décrit plus haut.

Incitatifs structurels

On constate ici que les avis sont nettement partagés. Les scénarios proposés, pourtant proches de la réalité, sont souvent jugés comme peu fréquents, à l'instar de l'exemple suivant: « *Germaine fait régulièrement des copies d'informations des plans financiers de l'entreprise sur un disque dur externe qu'elle ramène chez elle le soir. Selon elle, l'entreprise ne peut la retracer* ». 72 % des répondants estiment que cela n'arrive que ponctuellement ou rarement. Pour ce même item, l'ensemble des répondants trouve ce comportement inacceptable ou totalement inacceptable. Nous remarquons que la rareté d'un événement semble aller de pair avec sa gravité, ce qui pourrait refléter la banalisation de certains comportements dont la fréquence est plus élevée, par contraste avec des incidents plus ponctuels. La nature des informations pourrait aussi déterminer la gravité perçue en cas de vol, toutes choses égales par ailleurs.

La rareté d'un événement semble aller de pair avec sa gravité, ce qui pourrait refléter la banalisation de certains comportements dont la fréquence est plus élevée.

Nouvelles technologies

Les outils technologiques en eux-mêmes ne semblent pas, à première vue, représenter un facteur de risque disproportionné dans le vol de données et d'informations en interne. Les répondants estiment aussi fréquent de copier sur une clé USB des informations que de les copier en version papier (66 % contre 51 %), et trouvent dans les deux cas qu'il s'agit de comportements inacceptables pour 74 % d'entre eux. En revanche, l'envoi de courriers électroniques professionnels avec des fichiers joints est considéré comme fréquent par 79 % des participants, et est jugé inacceptable du point de vue de la sécurité dans seulement 27% des cas. Nous retrouvons pour cet item le constat fait précédemment sur la corrélation positive entre la fréquence et la tolérance.

Les outils technologiques en eux-mêmes ne semblent pas, à première vue, représenter un facteur de risque disproportionné dans le vol de données.

Risques

La moitié des répondants estime peu probable, voire non probable, que l'entreprise découvre que des informations ou des données aient été subtilisées en interne. Dans le cas contraire, 57 % des répondants pensent que la personne impliquée encourt un licenciement. Il apparaît que le risque est davantage pris en compte à travers la probabilité d'être découvert (rare) plutôt qu'en fonction de la gravité des conséquences que subirait la personne concernée (licenciement).

Climats éthiques de travail

Les résultats empiriques semblent confirmer qu'un climat de travail placé sous le signe de l'éthique a une influence sur le vol de données et d'informations en interne. Autrement dit, plus l'entreprise valoriserait des comportements

éthiques par la mise en place de politiques et de directives claires et par une préoccupation pour le bien-être de ses employés, moins ces derniers seraient enclins au vol de données et d'informations, et par extension à des comportements « antisociaux ». Les répondants ont en effet évalué leur milieu de travail de manière assez positive. Pour 57 % d'entre eux, les employés sont conscients des enjeux éthiques de l'entreprise et pour environ 65 %, le pouvoir est moins valorisé que l'honnêteté par les membres de l'organisation. Les réponses à l'échelle « climats éthiques de travail » semblent partiellement liées aux réponses concernant le constat du vol d'informations.

Un climat de travail placé sous le signe de l'éthique a une influence sur le vol de données et d'informations en interne.

Ainsi, 50% des personnes estimant que la malchance de certains collègues est perçue avec indifférence par leur milieu de travail ont répondu avoir eu connaissance d'un vol de données et d'informations en interne, alors que 58 % des personnes ayant considéré que ce n'était pas le cas n'ont jamais eu connaissance d'un vol d'informations et de données en interne. Cette relation est significative et d'ampleur moyenne ($p=0.015$; Vde Cramer = 0.432). De la même façon, environ 63 % des personnes plaçant l'honnêteté au-dessus de l'autorité dans leur milieu de travail ont répondu n'avoir jamais constaté de vol de données et d'informations en interne ($p<0.05$).

Tricherie

Cependant, alors que les répondants déclarent évoluer dans un climat de travail plutôt positif, l'échelle de « tricherie » montre que les individus estiment que les employés semblent privilégier leurs intérêts propres (entre 60 et 75%). Ces résultats confirment l'hypothèse de Demeulenaere (2003) : même si les individus adhèrent aux règles communes, ils estiment que les autres privilégient leurs propres intérêts et qu'ils sont ainsi avantagés par ce manque de scrupules. Ce résultat peut paraître étonnant, car les deux échelles corrèlent de manière non négligeable ($r=0.631$; $p<0.01$). Il est donc utile de noter l'importance des représentations que se fait un individu de son milieu de travail. Même s'il estime que ce dernier est favorable, il reste méfiant quant au respect des règles par les autres, ce qui le conduit donc parfois à enfreindre les règles sous le prétexte que les autres ne les suivent pas. On voit que la confiance accordée reste relativement faible et susceptible d'être révoquée de manière ponctuelle.

La solidarité interne des employés constitue un obstacle non négligeable à l'identification précoce des cas de vols d'informations.

Norme

Conformément aux hypothèses de la littérature, les auteurs de vols peuvent raisonnablement espérer échapper à une dénonciation et à des sanctions, même dans les configurations où leurs activités sont découvertes par des employés qui désapprouvent celles-ci. La solidarité interne des employés constitue selon nos données un obstacle non négligeable à l'identification précoce des cas de vols d'informations. Environ 64 % des répondants estiment ainsi que les employés sont conscients de ce qui est autorisé ou non sur le lieu de travail. Pour l'ensemble des items de cette échelle évoquant des scénarios de vol de données et d'informations, entre 76 et 95 % des individus perçoivent ces comportements comme inaccep-

tables, mais près de 60 % pensent par ailleurs que la probabilité que la personne soit dénoncée est peu probable, voire non probable.

Pression économique

La très grande majorité des participants (89%) trouve inacceptable d'utiliser les données et les informations de l'entreprise comme moyen d'obtenir des ressources financières supplémentaires. Face à cet aspect, les répondants jugent que ce type de configuration n'arrive que ponctuellement ou rarement, même si 48 % d'entre eux admettent que la pression économique et sociétale est suffisante pour pousser les individus à envisager d'autres moyens d'enrichissement que leur salaire régulier afin d'augmenter de manière ostensible leur pouvoir d'achat.

Satisfaction

L'échelle de satisfaction nous permet de dégager les cinq principales causes d'insatisfaction qui expliqueraient le vol de données et d'informations en interne.

- Le manque de reconnaissance pour le travail effectué **59 %**
- Le manque de stabilité de l'emploi **59 %**
- Les mauvaises conditions de travail **56 %**
- Les faibles possibilités d'avancement **50 %**
- Le faible sentiment d'accomplissement **50 %**

À l'inverse, le manque d'autonomie au travail ou des relations insatisfaisantes entre collègues ne sont pas, selon les répondants, des raisons qui incitent les individus à utiliser des informations et des données appartenant à l'entreprise. Plus précisément, nous avons étudié la relation entre les réponses aux items de l'échelle satisfaction et l'item concernant la constatation d'un vol de données et d'informations en interne. Par ailleurs, nous avons constaté une corrélation non négligeable entre le score global à l'échelle de satisfaction et celui à l'échelle de pression économique ($r = 0.571$; $p<0.01$), ce qui pourrait s'expliquer par le fait qu'en situation d'incertitude économique (comme la crise financière que traversent actuellement les pays développés), les causes d'insatisfaction telles que l'instabilité professionnelle ou des niveaux de rémunération jugés insuffisants sont ressenties d'autant plus intensément, ce qui aurait pour conséquence d'augmenter les risques de vols.

Les répondants ont du mal à percevoir le préjudice subi par les entreprises lors du vol de données et d'informations.

Inhibition

L'analyse des résultats obtenus pour le facteur d'inhibition révèle que les répondants ont du mal à percevoir le préjudice subi par les entreprises lors du vol de données et d'informations. En effet, alors que 79 % des répondants associent ce type d'incidents à une victimisation individuelle, seuls 50 % envisagent les organisations comme des victimes. Malgré tout, ils sont entre 90 et 95 % à estimer que ces agissements sont graves. Par ailleurs, on constate une corrélation entre le fait d'avoir eu connaissance de vols d'informations au sein de son entreprise et la prise en compte des effets individuels ($p = 0.05$). Des efforts importants restent donc à accomplir afin de sensibiliser cadres et employés aux répercussions désastreuses des vols d'informations sur le fonctionnement et la survie de l'organisation.

Participation à la création

Les données obtenues pour cette dimension infirment notre hypothèse concernant la participation à la création, dans laquelle nous avancions l'idée que l'intensité de l'implication dans un projet ou

dans la création d'une connaissance favorise le sentiment d'appropriation des informations associées et par extension, le vol de propriété intellectuelle. En effet, deux scénarios présentés aux répondants obtiennent des scores de fréquence et de tolérance élevés. Il s'agit dans le premier cas d'un employé qui utilise dans un nouvel emploi une méthode déposée de tri de base de données élaborée par un ancien collègue, et dans le second cas, d'un employé se servant d'informations protégées provenant d'un emploi précédent afin d'améliorer les performances de l'entreprise dans laquelle il travaille, sans spécialement détenir le poste approprié. Ces scénarios sont présentés comme fréquents par 65 et 70 % des répondants, et sont jugés acceptables par 49 et 66 % d'entre eux.

> **Les individus ont tendance à se montrer aux chercheurs sous un jour plus favorable que ce à quoi l'on peut s'attendre.**

Biais de désirabilité sociale

Comme dans de nombreuses études traitant de sujets dits « sensibles », nous avons été confrontés au biais de désirabilité sociale qui apparaît lorsque l'on collecte des données de manière auto-révélée. En effet, les individus ont tendance à se montrer aux chercheurs sous un jour plus favorable que ce à quoi l'on peut s'attendre. Ce biais est d'autant plus prononcé lorsque l'étude aborde des sujets qui pourraient embarrasser les répondants. Pour cette raison et afin de contrôler notre étude, nous avons ajouté dans le questionnaire une échelle mesurant ce biais. Malgré la confidentialité et l'anonymat des données collectées, les résultats montrent un biais de désirabilité sociale assez fort. En effet, le score moyen de notre échantillon à cette échelle est de 5,167 alors que le score moyen de l'échelle est de 6,5. Ceci indique que les personnes ayant répondu au questionnaire ont choisi les réponses socialement valorisées même si elles ne correspondent pas tout à fait à la réalité. Nous estimons donc à la vue de ce résultat que les individus ont pu sous-estimer les comportements indésirables évoqués dans le reste du questionnaire.

Nous croyons que ce score à l'échelle de désirabilité sociale démontre la sensibilité du sujet abordé. Nous percevons une crainte résiduelle chez les participants lorsqu'on leur demande de répondre sincèrement des questions qui traitent de déviance organisationnelle. Ceux-ci ont exprimé à travers les résultats une appréhension vis-à-vis des personnes qui pourraient avoir accès à leurs réponses, malgré les garanties de confidentialité et d'anonymat offertes par les chercheurs. Ces limites illustrent les raisons pour lesquelles ce type de travaux sur le vol d'informations et de données, notamment en interne, reste marginal en criminologie ou en sociologie du travail.

Conclusion

Les premières analyses semblent démontrer une prise de conscience de la part des répondants concernant le vol de données et d'informations en interne. Cependant, on remarque que ces derniers ont souvent eu tendance à dénoncer les comportements jugés peu fréquents, ce qui correspond à un engagement limité autour de cette problématique. À la vue de ce que nous démontrent la littérature et l'actualité, nous estimons au contraire que ces comportements sont bien plus répandus que les participants n'ont bien voulu l'admettre, ce que semblent confirmer les résultats inférieurs au score anticipé sur l'échelle de désirabilité sociale.

Nos analyses suggèrent que des mécanismes de prévention efficaces ne devraient pas uniquement se concentrer sur des solutions technologiques telles que le chiffrement des données ou le

déploiement de systèmes complexes de gestion des accès, comme l'un d'entre nous l'avait déjà souligné en matière de perte et de vol des données personnelles dans les organisations (Dupont, 2010). Les programmes destinés à lutter contre le vol d'informations doivent aussi s'appuyer sur les grands principes de la prévention situationnelle que sont la réduction des risques (des mécanismes de détection et de sanction accrus), l'augmentation des efforts (une accessibilité graduelle aux informations en fonction des besoins), la réduction des provocations (une meilleure prise en compte des conditions et du climat de travail) et la suppression des excuses (sensibilisation aux préjudices subis par l'organisation, tolérance réduite à la complicité tacite et mise en place de mécanismes de conformité aux règles de l'organisation). L'outil que nous avons élaboré permet de dresser à partir de données recueillies auprès des cadres et des employés un diagnostic complet des risques auxquels est confrontée une organisation, et d'identifier les domaines prioritaires d'intervention. Sans cette connaissance, et à défaut d'adopter l'approche intégrée des risques qui en découle, les organisations seront incapables de garantir à leurs actionnaires et à leurs partenaires l'intégrité de leurs actifs informationnels. ■

Audrey Asseman,
chercheure associée au CICC
(Centre International de Criminologie Comparée)
& Benoît Dupont,
directeur du CICC

Bibliographie

Adams, J.S. (1965). Inequity in social exchange. In L. Berkowitz (Ed.), Advances in experimental social psychology (Vol. 2, pp. 267-299). New York: Academic Press.

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.

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

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

Dupont, B (2010). Les organisations: sentinelles aveugles de la sécurité des données personnelles? Sécurité et Stratégie, 3, p. 26-34.

Felson, M. (2002). Crime and everyday life. 3rd Edition. Thousand Oaks : Sage publications. 211p.

Greenberg, J. (1997). The Steal Motive: Managing the social determinants of employee theft. In Giacalone R. & 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.

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.

Jaffe G. et Nakashima E. (2011). Mental health specialist reocmmended wikileaks suspect not be deployed to Irak. The Washington Post. 2 février.

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

Merton, R.K (1938). Social Structure and Anomie. American Sociological Review 3, p. 672-82.

Nakashima E. (2010). With better sharing of data comes danger. The Washington Post. 29 novembre.

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

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.