



Fraude interne, malveillance interne : détection et gestion

Synthèse de la conférence thématique du CLUSIF du 4 juin 2009 à Paris

Les cas de fraude et de malveillance internes font régulièrement la Une des journaux. Ce phénomène touche tous les pays et n'épargne aucun type d'entreprises. Pourtant, aucune d'entre elles ne souhaite témoigner sur le sujet, constate Pascal Lointier, Président du Clusif et conseiller sécurité de l'information chez AIG Europe.

La fraude interne serait-elle « le dernier sujet tabou en entreprise » ?

La fraude interne est pourtant une réalité en entreprise. Les exemples ne manquent pas :

- « Un agent d'assurances soupçonné d'avoir détourné 450.000 euros » (AFP, 20090206)
- « Un employé de la HSBC écroué pour détournement de fonds de clients » [900k€] (AFP, 20090319)
- « Une employée de Cryospace Air Liquide détourne 13,5 millions d'euros » (AFP, 20090225)

Les modes opératoires de la fraude sont relativement simples. Il peut s'agir d'un « one shot » (un gros coup), de fraudes menées sur des actions répétitives de faible amplitude, du contournement d'une procédure ou encore la résultante d'un contrôle interne trop faible.

La malveillance se retrouve également dans de nombreuses affaires :

- New Jersey, novembre 2008 : un fonds de pension décide de licencier une dizaine de personnes... dont l'administrateur réseau. Ce dernier installe plusieurs *backdoors* menace de les activer et de médiatiser l'affaire.
- Virginie, janvier 2009 : un ingénieur informatique employé chez FannyMae

détruit par bombe logique 4.000 serveurs. Le préjudice se chiffre en millions de dollars.

En ce qui concerne la malveillance, les motivations sont variées, mais le plus souvent le fraudeur se retrouve pris dans une spirale infernale. Le frein psychologique reste généralement minime, en raison de l'aspect « immatériel » de l'acte.

Environ 80 % de la malveillance serait interne en entreprise, mais aucune société ne veut s'exprimer sur le thème. Pour quelles raisons ? Peut-être la superstition ☺, la non maîtrise, voire un sentiment de culpabilité pour les entreprises victimes qui verraient ainsi la démonstration d'une incompétence. De plus, le RSSI est souvent censuré par la Direction de la Communication qui veut limiter toute diffusion d'information sur ces aspects de la vie en entreprise. Ce blocage de la « communication » est peut être un reliquat de ces stratégies de sécurité par l'obscurantisme qui prédominaient auparavant, mais cette absence de communication n'est plus possible dans un monde d'interconnexion. Il faut donc que les RSSI et la Direction de la

Communication se rapprochent. Dans les années 90, une entreprise n'osait avouer qu'elle avait été contaminée par un virus informatique mais aujourd'hui, on s'en explique librement, efficacement. Fraude et sabotages internes devraient suivre la même évolution. De plus, la fraude étant aujourd'hui informatisée, les RSSI doivent collaborer davantage avec le département d'audit interne, fonctionnellement en

charge de la prévention et de la détection des détournements d'actifs financiers.

En ce qui concerne la prévention de la fraude, les RSSI doivent aussi faire face à un écueil culturel. S'ils durcissent la politique de gestion des identités et des comptes, cela peut aussi être interprété comme une remise en question du degré de confiance au sein de l'entreprise.

Francis Hounnongandji, Président ACFE, Chapitre France

Qu'est-ce que la fraude interne ? Il s'agit de l'utilisation de son emploi à un profit personnel en détournant des actifs ou des ressources de son employeur.

Selon le rapport de l'ACFE sur la fraude interne 2008, une étude réactualisée tous les deux ans par l'ACFE, le coût de la fraude serait en hausse continue. Elle représenterait, en 2008, 7 % du CA en moyenne d'une entité, soit deux points de plus qu'en 2006.

Selon l'enquête publiée en avril 2009 par l'ACFE sur l'impact de la récession sur la fraude interne :

- 55 % des répondants estiment que la fraude est en hausse par rapport à l'année précédente et 49 % estiment que son impact est également plus important.
- 88 % prévoient une recrudescence des cas de fraude sur l'année à venir.
- 70 % classent les détournements d'actifs provenant des employés comme les cas de fraudes les plus fréquents à venir.

Le détournement d'actifs serait, toujours dans le rapport 2008, la fraude la plus courante, suivi de la corruption et de la manipulation des comptes. Néanmoins, le maquillage des comptes a un impact beaucoup plus important pour l'entreprise, car il implique généralement le top management. Le détournement d'actifs est, quant à lui, le plus souvent la résultante de petites actions émanant d'employés. Dans le calcul, certains coûts sont immatériels et

ne peuvent être estimés, comme l'impact sur l'image de l'entreprise.

Quels sont les moyens de détecter la fraude ? Pour l'ACFE, la dénonciation reste le meilleur moyen de détecter la fraude (46,2 %), suivi par le contrôle interne (23,3 %), le hasard (20 %), l'audit interne (19,4 %), l'audit externe (9,1 %), et enfin celles qui sont notifiées par la police (3,2 %). Cependant, même en cas de détection, il n'est pas toujours facile de dénoncer une fraude en raison des pressions subies.

Quelles sont les causes de la fraude ? La faiblesse du contrôle interne, une culture permissive, le contournement des contrôles existants, la pression du marché sur le management, surtout en période de crise... Le passage à l'acte a plus de risques de se faire si trois conditions sont réunies : une opportunité, une pression et une capacité d'autojustification. La fraude se fait le plus souvent par opportunité. Elle concerne surtout les personnes qui se sentent lésées, celles qui vont quitter l'entreprise... Plus la pression augmente, plus les objectifs des acteurs économiques deviennent irréalistes, les faiblesses des systèmes de contrôle interne s'accroissent, la loyauté entre les personnes et les organisations diminue, les moyens alloués à lutter contre la fraude aussi.

Estelle Dossin, psychologue clinicienne, Ministère de l'Intérieur, DFPN

Que se passe-t-il dans la tête d'une personne qui va voler ? De quelle manière intégrons-nous les notions d'interdit ? Pour y répondre, il est nécessaire de s'intéresser au psychisme de chacun. C'est à l'issue de la résolution du complexe d'Oedipe que le Surmoi se crée. Il s'agit d'une instance psychique qui détermine la notion de loi, de bien et de mal, que l'on compare généralement au « gendarme » du psychisme. Le surmoi détermine notamment les notions de Limite et d'Interdit. L'interdit représente la digue de contention qui contient la pulsion. Cette digue va être plus ou moins forte selon les individus, selon la qualité de la construction du surmoi. Quand on est mal « Surmoisé », la digue de l'interdit cède, la pulsion passe au travers. C'est le passage à l'acte.

Estelle Dossin distingue 4 types de fraudeurs :

- **Le vengeur** : il va utiliser l'acte frauduleux comme moyen de vengeance personnelle. Il n'est pas dangereux tant qu'on ne l'embête pas. Ce sujet hypersensible fait preuve d'une fragilité narcissique. Il est sensible à la critique et observe des difficultés dans ses relations interpersonnelles. En entreprise, si l'exigence est trop forte, il se sentira menacé et répliquera, avec pour objectif d'atteindre l'employeur. Pour essayer d'anticiper ce type d'acte, il est important d'observer au préalable la résistance au stress et à la frustration d'un employé.

- **Le malveillant** : il utilise l'acte frauduleux comme acte de malveillance délibérée. C'est le plus dangereux car sa malveillance est agie, sans le moindre scrupule. Le malveillant opère par sa rage de réussir, à n'importe quel prix. D'apparence sympathique et affable, il va agir via la séduction et toutes autres formes de manipulation mentale. Il est difficilement décelable et se caractérise par un fort potentiel de nuisance.

- **Le fraudeur occasionnel et/ou fraudeur économique par nécessité** : dans le premier cas, c'est l'occasion qui va faire surgir la pulsion. Le plus souvent, la fraude est mineure et l'acte n'est pas vraiment culpabilisé, la personne étant convaincue que ce n'est pas si grave. Dans le second cas, c'est la peur du manque qui agit. La personne va rationaliser son acte par la nécessité. Dans ces deux cas, le danger majeur pour l'entreprise sera le risque de propagation, de répétition et le nombre de personnes à le faire.

- **Le cybercriminel et cyberfraudeur** : c'est un profil particulier, puisque ce n'est pas son organisation psychique qui détermine son passage à l'acte. Il a des connaissances poussées en informatique et est conscient de sa maîtrise. La cible se caractérise essentiellement par son ignorance en la matière. L'attaque est d'autant plus rentable que l'effort est moindre. Le cyberfraudeur ne culpabilise pas, car la victime n'a pas de visage, pas d'identité. De plus, le risque légal n'est pas beaucoup plus important que le risque moral. Un cybercriminel agit uniquement dans la sphère informatique qui l'encourage et le protège. Il n'ira sans doute jamais voler un sac à main.

La fraude est peu ou pas prévisible. Les motivations et les profils sont très variables. La prévention s'avère donc difficile. Pour Estelle Dossin, le recrutement psychologique permet de déterminer la résistance à la frustration, les capacités surmoiques de l'individu et de sa gestion du stress. Le management humain s'avère également fondamental. Pour former et informer le personnel sur la fraude, mieux vaut faire appel à des personnes extérieures à l'entreprise, veiller à la communication et à l'environnement de travail.

Me Blandine Poidevin, Avocat au barreau de Lille et Paris, Jurisexpert

Comment peut-on réagir d'un point de vue juridique en cas de fraude et de malveillance ? Tout d'abord, la plainte pénale : elle peut relever d'un cas de vol, d'escroquerie, d'intrusion dans un système d'information, de contrefaçon ... Cependant, le dépôt de plainte s'inscrit dans un délai préalable de saisine éventuelle du Parquet de trois mois, sauf dans le cas d'infractions de presse. Dans une problématique de preuve, afin de prouver la mise en cause de telle personne, ce délai peut s'avérer problématique. C'est pourquoi il est possible de lancer une procédure non contradictoire d'ordonnance sur requête. En référence au décret du 24 mars 2006 sur la « conservation des données relatives au trafic », vous pouvez demander la communication des informations détenues par les FAI, opérateurs de téléphonie fixe et mobile, hébergeurs, éditeurs de forums, ...

Dans le cadre de la constitution des preuves, on peut également recourir à un constat d'huissier. Il s'avère utile lorsqu'il y a des choses concrètes à constater rapidement dans l'entreprise. Pour que le constat d'huissier (TGI Nanterre, 24 mai 2000) soit valable, il doit être fait dans les règles : l'ordinateur ne doit pas être en réseau, la mémoire cache de l'ordinateur doit être vidée et les fichiers Internet temporaires, cookies, historique des navigateurs effacés. L'adresse IP du site consulté doit être vérifiée, ainsi que la connexion à un serveur Proxy. L'huissier doit décrire le cheminement de la page d'accueil du site jusqu'à la page litigieuse. Si l'ensemble de ces éléments n'est pas respecté, le constat d'huissier sera nul. Il ne s'agit pas de constituer une preuve technique mais une preuve juridique. En outre, depuis 2003, le constat doit se faire à partir d'un ordinateur situé dans les locaux de l'huissier.

Luc Vignancour, Directeur adjoint, Marsh S.A.

Certains contrôles peuvent également être effectués sur le poste du salarié, dans la mesure où les salariés sont informés au préalable des dispositifs de contrôle mis en œuvre. A ce sujet, il est parfois difficile de trouver l'équilibre entre le contrôle des salariés et le respect de leurs droits, la jurisprudence évoluant régulièrement en la matière (Arrêt Nikon 2001, Arrêt Cathnet 17 mai 2005, Cass. Soc. 9 juillet 2008). Pour éviter ce type d'incident, la charte informatique et son contenu apparaissent essentiels pour l'entreprise et peut même s'avérer décisive en cas de jugement (Cass. Soc. 21 décembre 2006).

Le rôle de l'administrateur réseau doit également y être clairement défini. Les administrateurs réseau assurent le fonctionnement normal et la sécurité du système informatique, ont accès à des informations personnelles relatives aux utilisateurs. Mais s'interdisent toute divulgation d'informations connues dans le cadre de leur mission, dès lors qu'elles ne remettent pas en cause le fonctionnement technique ou la sécurité des applications, ou l'intérêt de l'employeur. L'obligation de confidentialité doit être rappelée dans le contrat de travail et la charte informatique.

Parmi les perspectives futures, un projet de loi « sécurité intérieure » a été présenté le 27 mai dernier. Il prévoit la création d'un délit d'usurpation d'identité sur Internet qui pourra être réprimé pour préjudice moral, même en l'absence de dommage financier. Il devrait également permettre aux entreprises de déployer des systèmes de vidéosurveillance pour prévenir les atteintes aux biens dans des lieux particulièrement exposés, même s'ils ne sont pas particulièrement menacés par des actes de terrorisme.

Lorsqu'une fraude arrive, il existe un moyen de récupérer une partie des pertes que subira l'entreprise, même si l'auteur de la fraude n'est pas identifié : l'assurance.

La fraude ou malveillance est un risque assurable car sa réalisation est indépendante de la volonté de l'assuré et son impact est mesurable et quantifiable..

L'assurance va s'organiser autour de deux types de garantie :

- le risque de fraude (détournement de fonds et/ou de biens),
- le risque de malveillance (action qui perturbe le bon fonctionnement de l'entreprise).

La fraude

Comme tout sinistre, la fraude est définie par des faits générateurs et des impacts. Parmi les principales causes, on retrouve l'escroquerie, l'abus de confiance, les faux et usage de faux, le vol... Pour ce qui est des conséquences, la perte va se matérialiser par la disparition des biens (marchandises ou valeurs) dont l'assuré était propriétaire. L'expertise s'articule principalement autour de l'analyse des documents comptables pour déterminer le montant de la perte. Toutes les fraudes commises par le même auteur seront considérées comme faisant partie du même sinistre.

D'autres facteurs sont à prendre en compte: certains contrats ne couvrent la fraude que si l'auteur ou l'un de ses complices en a tiré un profit personnel, de plus les conditions de garantie peuvent différer selon que l'auteur est un employé ou un tiers.

Le contrat a pour objet de couvrir les pertes de l'Assuré et non les pertes que fait

subir l'assuré à un Tiers. Enfin, la fraude doit généralement être découverte dans les cinq années suivant sa réalisation pour prétendre à une couverture.

Certaines fraudes ne sont pas couvertes : celles commises par les dirigeants ou mandataires des entreprises, par un employé récidiviste, lors de la délivrance d'un crédit ou au cours d'opérations sur les marchés, et celles dont le mécanisme ne peut pas être démontré. Dans tous les cas, c'est à l'Assuré de démontrer qu'il est victime d'un sinistre et qu'il a subi une perte. De plus, il faut savoir que le dépôt de plainte est souvent requis.

La malveillance

En ce qui concerne la malveillance, les causes sont généralement peu précises. On parle le plus souvent « d'actes de malveillance » mais les références aux articles du code pénal relatifs à l'Atteinte aux Systèmes de Traitement Automatisé de Données est de plus en plus fréquente. Pour être assurables, les impacts doivent être quantifiables et valorisables, ce qui n'est pas évident quand on parle de disponibilité, d'intégrité, de confidentialité et de traçabilité. Pour quantifier un acte de malveillance, on regarde les frais engagés par l'entreprise pour réparer la malveillance et maintenir son activité économique ainsi que les pertes éventuelles de chiffre d'affaires. L'assurance permet donc de transférer chez un assureur les pertes supportées et les coûts engagés. Cependant, la quantification de ces pertes doit être faite par l'entreprise sinon il n'y a pas d'assurance possible.

Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF

<http://www.clusif.asso.fr/fr/infos/event/#conf090604>.