

LA LETTRE DU RISQUE CLIENTS

Lundi 22 juin 2015

AU SOMMAIRE

DOSSIER

- **La fraude : nouveau fléau des entreprises françaises ?** p.1
- **Ils témoignent : Groupe Westpoint / Louis Vuitton** p.4
- **Etude EH / DFCG 2015 sur la fraude externe** p.6
- **Expertise : analyse de l'étude** p.7

La fraude : nouveau fléau des entreprises françaises ?

Usurpations d'identité, cyber-attaques, détournements de fonds ou de marchandises... Ces nouveaux fléaux s'abattent en masse sur les entreprises françaises depuis moins de cinq ans. Comment y faire face et se prémunir, face à des escrocs de mieux en mieux renseignés et organisés ? Parler du risque de fraude n'est pas toujours chose aisée, surtout lorsqu'il concerne la vie interne de l'entreprise. L'occasion de lever un tabou et de mettre en place des mesures de protection pour protéger au maximum les actifs de l'entreprise.

Les entreprises savent appréhender une multitude de risques, qu'ils concernent leur chaîne d'approvisionnement, leur environnement, ou la protection de leurs transactions financières. Mais il existe aussi d'autres menaces, comme le risque d'escroquerie ou le détournement d'actifs. Ces fraudes ne sont pas forcément nouvelles en tant que tel. Par contre, l'ampleur de ce phénomène est quant à lui relativement récent et touche tout type d'entreprise. Le nombre de fraudes subies par les entreprises françaises a presque doublé depuis 2009. 55% d'entre elles en ont été victimes au cours des 24 derniers mois¹. 17% des DAF déclarent avoir connu plus de 10 tentatives de fraude externe dans l'année écoulée.

La fraude : quelle définition ?

Il n'existe pas de réelle définition juridique de la fraude. Retenons que la fraude est un acte commis dans l'intention de nuire et d'en tirer un profit illicite. Pour définir une fraude, il faut donc qu'il y ait volonté de commettre un acte en violation avec un cadre, et un préjudice au détriment de quelqu'un ou à son propre bénéfice. Ainsi, le collaborateur qui efface par mégarde une base de données ne commet pas une fraude, mais bel et bien une erreur. Il n'avait pas l'intention de le faire pour nuire à l'entreprise ou pour en tirer profit.

Plusieurs types de fraude existent, qu'elles soient « externes » à l'entreprise, c'est-à-dire commises par un tiers, ou « internes », réali-

EULER HERMES



Par **Laura Flandin**, responsable du marketing produit, Euler Hermes France

sées par un collaborateur. Citons par exemple le détournement de fonds, le détournement d'actifs – quand un collaborateur vole de la marchandise ou des matériaux pour les revendre à son propre bénéfice – l'escroquerie, le faux et usage de faux, l'abus de confiance... 85% des fraudes dans les entreprises sont commises par des collaborateurs dans le cadre de leur fonction². « On ne l'appréhende pas toujours sous cet angle mais la corruption est également une fraude. Un collaborateur qui touche de l'argent pour préférer un fournisseur plutôt qu'un autre, peut in fine coûter beaucoup d'argent à l'entreprise » explique Laura Flandin, responsable du marketing produit chez Euler Hermes France.

Les cyber-fraudes connaissent elles-aussi un nouvel élan, menaçant les systèmes informatiques de l'entreprise et donc l'accès à ses données, y compris les plus confidentielles.

Plusieurs conséquences sont alors possibles : les « pirates » peuvent se connecter aux systèmes dans le but de détruire des données, ou d'en accumuler pour mieux connaître leur « proie » et parvenir à détourner de l'argent. Certains parviennent même à se connecter aux systèmes téléphoniques pour

passer des appels surtaxés. La facture peut alors être salée !

Pour la première fois dans son baromètre annuel des risques, Allianz affichent les risques de cyberattaques et de fraudes dans le top 10 des risques auxquels sont confrontées les entreprises.

Se méfier de l'usurpation d'identité

L'usurpation d'identité arrive en tête des tentatives de fraudes subies par les entreprises cette année³. Les « faux acheteurs », les « faux fournisseurs », ou « les faux présidents » ont le vent en poupe ! L'imagination des escrocs est sans limite. Ils sont très habiles, font preuve de fermeté, savent imiter les voix, faire pression en abusant de leur faux rapport hiérarchique, et savent aussi glisser des éléments personnels pour susciter la confiance de leurs interlocuteurs. L'escroc se fait alors passer très facilement pour le président ou le directeur administratif et financier d'une en-

treprise et, prenant prétexte d'une opération de croissance externe qui doit rester confidentielle, exige le versement d'une somme importante sur le compte d'une banque étrangère. Autre cas de figure : le faux fournisseur prétexte un changement de RIB pour détourner des paiements... qui partent à l'étranger, en transitant souvent par plusieurs pays. Une autre arnaque consiste à usurper l'identité du client de l'entreprise : ce n'est qu'au moment de réclamer le paiement à son client « habituel » que celui-ci lui indique n'avoir jamais passé commande... et la marchandise est déjà loin ! « C'est une pratique courante au moment des fêtes de fin d'année, en visant les entreprises du secteur de l'agro-alimentaire et notamment les denrées périssables », commente Eva Sebban, responsable du recou-

virement export chez Euler Hermes France.

« Les montants tournent en moyenne autour de 10 000 euros mais j'ai eu récemment un cas frauduleux de livraison de marchandises qui atteignait 400 000 euros ! Une perte sèche qui peut vraiment fragiliser l'entreprise. » Dans ces cas d'usurpation d'identité, le dépôt de plainte permettra d'ouvrir éventuellement une enquête et de faire reconnaître

la fraude. Mais les espoirs de récupération sont quasi-nuls. « En 10 ans, les choses ont beaucoup changé. On voyait des cas similaires surtout sur le marché domestique et il ne s'agissait que de quelques dossiers dans l'année. J'en ai désormais tous les mois. A chaque fois, nous avons à faire à des bandes très bien organisées, avec des modes opératoires rodés et ils ciblent tout type d'entreprise. A chaque fois, les perspectives de récupération sont nulles : les auteurs de la fraude sont difficilement identifiables et ils ont organisé leur insolvabilité » ajoute Eva Sebban.

Des conséquences lourdes

La fraude coûte cher aux entreprises. Elle impacte directement leur trésorerie, à hauteur des sommes détournées. Mais la fraude est aussi souvent médiatisée, comme les exemples de Michelin, victime de faux ordres de virement, du club de football de Marseille, l'OM, qui s'est

Le nombre de fraudes subies par les entreprises françaises a presque doublé depuis 2009. 55% d'entre elles en ont été victimes au cours des 24 derniers mois.

fait dérober plus de 700 000 euros, ou encore, plus grave, un fabricant de maïs, fournisseur du Géant Vert, qui a perdu 17 millions d'euros par un détournement frauduleux... L'entreprise subit alors de surcroît les effets négatifs en termes d'image et doit mettre en place un processus de communication de crise. Certaines situations de fraude interne peuvent également être traumatisantes pour l'entourage.

Détecter les situations à risque

Les professionnels du risque de fraude le répètent : il n'y aura jamais de risque zéro, mais certaines bonnes pratiques peuvent limiter la casse. Il est tout d'abord primordial de détecter les situations à risques : être attentif aux changements d'interlocuteurs, aux demandes de livraison à de nouvelles adresses, ou des adresses suspectes, à un client qui achèterait des marchandises dans un secteur qui n'est pas le sien (une entreprise qui achèterait des vêtements de marque alors qu'elle agit « normalement » dans le secteur du BTP par exemple). « Certains escrocs louent des hangars au mois ou à la journée, uniquement pour réexpédier la marchandise détournée », avertit Eva Sebban. Les équipes commerciales sont en première ligne pour détecter l'usurpation d'identité. Elles peuvent contribuer à vérifier l'identité du client, ou confirmer qu'il s'agit bien de leur contact habituel. Echanger une carte de visite lors d'un salon professionnel ne suffit pas. Les cartes sont facilement falsifiées... Sans céder à la paranoïa, les entreprises peuvent ajuster leurs procédures internes et former leurs commerciaux pour avoir les bons réflexes comme envoyer une confirmation de commande avant de livrer la marchandise ou faire quelques recherches sur l'identité de leur prospect.

Tous les collaborateurs doivent être sensibilisés

Prendre conscience que ces risques sont à la porte de l'entreprise et savoir comment réagir : c'est aujourd'hui probablement le meilleur rempart à la fraude. Pour mettre en place une véritable politique de prévention, la sensibilisation des équipes est primordiale, surtout quand on observe que les fraudes sont déjouées en majorité grâce à un bon dosage de procédures de contrôle et de réactions humaines. Le directeur financier joue ici un rôle central dans ce dispositif, non seulement pour optimiser les procédures existantes, former directement les collaborateurs

en prise directe avec les enjeux financiers de l'entreprise, mais aussi leur comité de direction. 80% des entreprises françaises affirment que la fraude est reconnue comme une menace importante par la direction générale⁴, mais seules 28% d'entre elles disposent d'une cartographie des risques. C'est donc aujourd'hui un enjeu stratégique qui doit permettre à l'entreprise d'évaluer ses points de vulnérabilité et de se doter d'outils d'alerte ou de modifier certaines pratiques. « Le risque de fraude permet de remettre à plat certains fonctionnements et de se poser la question de sa sécurité et de son efficacité. Il peut, en outre, créer une certaine transversalité entre des directions financières, commerciales, de l'audit ou des systèmes d'information », témoigne Sébastien Hager, souscripteur d'assurance fraude pour Euler Hermes France.

Prévention + protection = sécurité!

Face à l'ingéniosité et la créativité des escrocs, la prévention ne peut malheureusement pas tout. En dépit des mesures de protection mises en place dans les entreprises, 20% n'ont pas réussi à déjouer toutes les tentatives de fraude auxquelles elles étaient confrontées cette année⁵. Il existe des assurances qui couvrent tout ou partie de ce risque de fraude mais elles sont souvent méconnues. 81% des entreprises françaises ne connaissent pas encore l'existence de ces assurances anti-fraude qui permettent d'indemniser l'entreprise, en fonction d'une couverture choisie, et prend en charge aussi bien les pertes financières directes, que l'impact éventuel sur la réputation de l'entreprise et une contribution aux frais de procédure judiciaire engagés. La plupart des entreprises du CAC 40 sont assurées, mais les PME restent très faiblement équipées. L'assureur-crédit Euler Hermes propose depuis le début de l'année une assurance fraude adaptée aux PME, couvrant à la fois la fraude interne, externe et la cyber-fraude. « Nous proposons ce produit à nos clients en Allemagne depuis plus de 30 ans. Compte tenu de l'explosion des fraudes en France, nous avons décidé de commercialiser cette offre ici dès cette année », relate Laura Flandin. « La conséquence d'une escroquerie sur la trésorerie de l'entreprise est la même que pour un impayé. Une assurance pour se prémunir de ce type de risque contribue à une gestion saine de l'entreprise. » Informée, organisée, protégée, l'entreprise se donnera ainsi les moyens de réduire la fraude et de barrer la route aux escrocs. ■



Eva Sebban, responsable du recouvrement export, Euler Hermes France



et Sébastien Hager, souscripteur d'assurance fraude, Euler Hermes France

1 Etude PwC 2014

2 Etude EY 2014

3 Etude Euler Hermes / DFCG 2015

4 Etude Euler Hermes / DFCG 2015

5 Etude Euler Hermes / DFCG 2015

Ils témoignent

Westpoint : quand l'assurance fraude vient compléter les mesures de prévention déjà en place



Jérôme de La Rivière,
président, Westpoint

Westpoint, société familiale basée à Bordeaux et créée en 1875 est spécialisée dans le négoce de climatisation et d'électroménager vers plus de 95 pays tropicaux. Son Président, Jérôme de La Rivière, revient sur le cas de fraude que l'entreprise a subi l'an dernier.

En dépit des mesures de prévention existantes, votre entreprise a subi à une fraude l'an dernier. Comment y avez-vous fait face ?

En 2014, à l'occasion d'un contre-appel de notre banque, nous nous sommes rendus compte que notre compte – qui n'avait jamais été autorisé au découvert et qui était à l'époque créditeur de 500 000 – avait été mis dans une position débitrice de 1,5 million €. Ceci s'est fait sans qu'aucune personne de la société ne donne d'instruction en ce sens à la banque et sans qu'aucune intrusion n'ait eu lieu dans nos systèmes. Nous étions pourtant particulièrement outillés sur les procédures de lutte contre la fraude notamment sur les paiements de nos clients et de nos fournisseurs puisque travaillant avec 95 pays à l'international, nous sensibilisons régulièrement notre personnel à ce risque de fraude. D'ailleurs, six mois auparavant, nous avons organisé un séminaire de protection de l'information à l'international pour nos commerciaux. Cela fait plusieurs années que nous avons pris le contrôle de notre filiale informatique responsable du développement

de nos logiciels afin de sécuriser nos sources et données informatiques contre les fraudes éventuelles. Dans le cadre de nos procédures, seuls nos commerciaux sont habilités à donner des ordres de paiement à la comptabilité et à la trésorerie. Par ailleurs, le changement éventuel d'un RIB client ou fournisseur ne peut s'opérer qu'avec l'accord du commercial en charge, du responsable pays et de moi-même. Malgré toutes ces dispositions, nous avons été victimes de ce vol et avons donc pris la décision de souscrire une assurance complémentaire spécifique contre la fraude afin de sécuriser notre cash en complément de celle déjà existante

en assurance-crédit sur la protection de notre poste client.

Quels conseils donneriez-vous pour se protéger de la fraude ?

De sensibiliser en permanence ses équipes sur le terrain, de mettre en place des procédures strictes et suivies du règlement clients et fournisseurs et d'assurer la traçabilité de tous les flux entrants et sortants de l'entreprise. Et de souscrire une assurance contre la fraude ! ■

Travaillant avec 95 pays à l'international, nous sensibilisons régulièrement notre personnel au risque de fraude.

Ils témoignent

Louis Vuitton : quand la lutte contre la fraude devient une responsabilité transverse dans l'entreprise

Un tandem DAF – Directeur du contrôle interne pour lutter efficacement contre la fraude ? Jean-Christophe Vincey, Directeur Financier EMEA, et Timothy de Chaisemartin, Directeur du contrôle interne et Organisation chez Louis Vuitton, témoignent de cette bonne pratique et de leurs échanges réguliers pour protéger les actifs de l'entreprise.

Quelles actions avez-vous mises en place pour lutter contre la fraude ?

JCV : Nous sensibilisons régulièrement nos directeurs de magasins au sujet de la fraude, en intégrant des éléments de prévention dans le manuel de gestion des magasins. Nous intégrons aussi ce thème dans des formations ou lors de réunions internes. Cette problématique doit être portée et comprise par le management local pour être combattue de façon efficace.

TdC : Les équipes changent : il faut donc renouveler ce type de sensibilisation de manière récurrente. Nous menons en parallèle une politique de prévention des conflits d'intérêt, pour que nos collaborateurs déclarent les cadeaux reçus et puissent à minima nous alerter de situations conflictuelles. Nous participons à un reporting mensuel des fraudes via la direction de l'audit interne du groupe LVMH. Cela permet d'avoir une veille permanente et partagée avec les différentes marques du groupe. Enfin, l'audit

interne n'intervient pas que dans le contrôle mais aussi dans la prévention, pour alerter les équipes sur les risques encourus et les aider à avoir les bons réflexes.

Quels conseils donneriez-vous pour se protéger de la fraude ?

JCV : Les procédures sont indispensables mais il ne faut pas oublier l'humain. Il est déterminant de rappeler régulièrement les règles de base, en faisant un effort de pédagogie et de communication. Il faut aborder ces sujets de manière simple et très opérationnelle.

TdC : La fraude est une responsabilité partagée dans l'entreprise avec les directions financières, commerciales et avec la direction des systèmes d'information qui fait régulièrement

des tests d'intrusion dans nos systèmes pour en mesurer la robustesse. La confidentialité des données est primordiale car il ne faut pas oublier que l'accès aux informations de l'entreprise facilite ensuite les actions des fraudeurs. ■

La confidentialité des données est primordiale car il ne faut pas oublier que l'accès aux informations de l'entreprise facilite ensuite les actions des fraudeurs.



Jean-Christophe Vincey,
directeur financier, EMEA,
Louis Vuitton



Timothy de Chaisemartin,
directeur du contrôle interne
et Organisation, Louis Vuitton

Étude Euler Hermes - DFCG 2015 Fraude : conséquences & enjeux pour l'entreprise

(mai 2015, 184 répondants, à 80% des DAF)



des entreprises ont été victimes (d'au moins) une tentative de fraude externe dans l'année écoulée



ont connu plus de 10 tentatives de fraude externe sur cette même période !



répondent qu'ils n'ont pas réussi à déjouer toutes les tentatives de fraude externe

TOP 5 DES TENTATIVES DE FRAUDES EXTERNES (rencontrées par les DAF*)

1



Fraude au président (60% d'entre eux)

2



Faux ordres de paiement (40% d'entre eux)

3



Modification des coordonnées fournisseurs

4



Recours à des virus (cyber attaque)

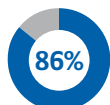
5



Fraudes aux tests SEPA

TOP 3 = Usurpation d'identité

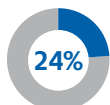
Les dispositifs ayant permis de déjouer les tentatives de fraude externe



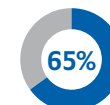
Réactions humaines



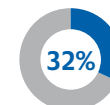
Procédures de contrôle interne



Dispositifs techniques



Procédures renforcées



Formations internes



Nouveaux logiciels

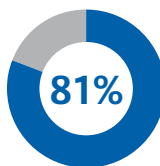
Les moyens mis en place pour lutter contre les attaques



80% répondent que la fraude est considérée comme une menace importante par la direction de l'entreprise et **90% des DAF** déclarent avoir sensibilisé leur comité de direction aux risques.

Pourtant **28%** seulement disposent d'une cartographie de leurs risques de fraude

et **38%** ont mené un audit sécurité de leur SI



des entreprises ne connaissent pas l'assurance contre le risque de fraude

(étude BVA / Euler Hermes 2014 - 600 répondants)

*DAF : Directeur Administratif et Financier.

www.eulerhermes.fr



EULER HERMES
Our knowledge serving your success*

A company of Allianz

Expertise / Analyse de l'étude

Avec plus de 20 ans d'expérience dans l'assurance fraude, Michel van Swieten, expert fraude chez Euler Hermes, commente les résultats de l'étude Euler Hermes / DFCG sur la fraude externe, menée pour la première fois cette année auprès de 200 DAF. Un phénomène qui connaît une augmentation sans précédent et qui fait l'objet d'une très forte médiatisation.

L'étude fait ressortir un véritable harcèlement des entreprises françaises. Les fraudeurs tentent plusieurs fois de suite... jusqu'à la faille ?

C'est exactement ça ! Les entreprises françaises sont victimes, les unes après les autres, de criminels en col blancs, qui enquêtent parfois très longtemps sur leurs « proies » et connaissent parfaitement les rouages internes. Ils cherchent des informations sur les réseaux sociaux, et parviennent à obtenir des données confidentielles en s'introduisant dans les systèmes d'information de l'entreprise. Ils tentent alors plusieurs fois de suite de détourner de l'argent, en usurpant l'identité du président, d'un fournisseur, d'un bon client... L'usurpation d'identité arrive clairement en tête des tentatives de fraude. Le recours à des virus, mentionné dans le top 5 des principales fraudes, est souvent un préalable, pour capter des informations sensibles. Ce phénomène, relativement récent, est piloté des groupes organisés très professionnels, qui œuvrent depuis l'étranger – souvent des pays d'où ils ne peuvent pas être extradés. Quoiqu'il arrive, ils ont évidemment organisé leur insolvabilité, la chance de récupération après une fraude est donc quasi nulle.

Comment se prémunir de ce type d'attaque ?

Pour que ce phénomène soit connu des

autorités, et qu'il soit ainsi mieux combattu, je conseille aux entreprises de porter plainte contre X, même lorsqu'il s'agit d'une tentative de fraude qui a été déjouée. Puis, il y a quelques bonnes pratiques à mettre en place, comme des systèmes de double signature ou de signature électronique. Mais les procédures ne peuvent pas tout ! L'intelligence et la vigilance des individus restent le meilleur rempart, et arrivent

d'ailleurs en tête des dispositifs permettant de déjouer une fraude, d'où l'importance de sensibiliser les équipes. Les escrocs connaissent souvent très bien les procédures internes et vont tout faire pour les contourner... Y compris parfois en utilisant les menaces ou le chan-

tage. Un collaborateur bien formé saura mieux détecter une opération inhabituelle, même si celle-ci respecte pour autant parfaitement les standards requis, et aura le réflexe de vérifier et d'informer sa direction en cas de doute.

Pourtant, la vigilance humaine n'est pas infaillible. Il n'y a donc aucune mesure pour atteindre le risque 0 pour l'entreprise ?

C'est sûr, les équipes peuvent changer, être moins sensibles au risque de fraude ou tout simplement se faire « avoir ». C'est pourquoi, au-delà de ces mesures de prévention, une protection contre ce type de risque me semble aujourd'hui indispensable pour protéger sa trésorerie. L'as-



Michel van Swieten,
expert fraude,
Euler Hermes

L'usurpation d'identité arrive clairement en tête des tentatives de fraude.

surance « EH Fraud Cover », distribuée par Euler Hermes depuis le début de l'année, s'adresse ainsi aux PME, en leur offrant un contrat très simple, couvrant la fraude interne, externe et la cyber-fraude. L'entreprise bénéficiera d'un accompagnement personnalisé dès la découverte du sinistre et pourra ainsi mieux appréhender le risque de fraude et protéger ses actifs en connaissant les bonnes pratiques en la matière.

L'étude se concentre sur le phénomène

très médiatisé de la fraude externe. On parle encore peu des fraudes internes. Un tabou ?

Oui, d'une certaine manière, il est plus difficile d'en parler pour un dirigeant, sans stigmatiser ou risquer de froisser ses collaborateurs.

La durée moyenne d'une fraude interne est de 18 mois avant d'être découverte et les chances de récupération sont là aussi très faibles.

Pourtant, il ne faut pas oublier que les fraudes internes déclarées sont moins nombreuses mais généralement plus sévères, notamment en raison de leur durée. La durée moyenne d'une fraude interne est de 18 mois avant d'être découverte et les chances de récupération sont là aussi très faibles. En guise de prévention, le dirigeant peut par exemple choisir d'en parler ouvertement par la mise en place d'un code d'éthique ou d'un plan anti-fraude. L'étude montre que le sujet de la fraude s'in-

vite déjà à l'ordre du jour de certains comités de direction. Il faut qu'il soit désormais mieux partagé au sein de l'entreprise car la France est en retard sur ces sujets comparativement à ses voisins européens. Le DAF a un vrai rôle à jouer dans cette évolution. ■

EULER HERMES

Euler Hermes France
1, place des Saisons
92 048 Paris La Défense Cedex
tél : + 33 (0)1 84 11 50 50
fax : + 33 (0)1 84 11 50 17
www.eulerhermes.fr

Si vous souhaitez contacter les auteurs de cette lettre, vous pouvez vous adresser à :

Sebastien Hager : sebastien.hager@eulerhermes.com
Laura Flandin : laura.flandin@eulerhermes.com



Supplément du numéro 1323 du 22 juin 2015
Option Finance - 10, rue Pergolèse 75016 Paris - Tél. 01 53 63 55 55
SAS au capital de 2 043 312 € RCB Paris 343256327
Directeur de la publication : Jean-Guillaume d'Ornano
Service abonnements : 10, rue Pergolèse, 75116 Paris - Tél. 01 44 84 80 45
Impression : Megatop - Naintre - N° commission paritaire : 0416 T 83896