FISCALITÉ, COMPTABILITÉ, DROIT

FRAUDE

Restez vigilant

OPTION FINANCE - 17 MAI 2016 - ASTRID GRUYELLE

Fraude

Si la fraude au président est désormais bien connue des entreprises, celles-ci doivent toutefois continuer à se montrer vigilantes. Pour parvenir à leurs fins, les escrocs élaborent en effet des scénarios de plus en plus complexes, en multipliant notamment les fausses identités. Afin d'y faire face, les directions financières ont tout intérêt à former régulièrement leurs équipes pour qu'elles acquièrent les bons réflexes, et à communiquer largement après chaque tentative frauduleuse.

L'imagination des fraudeurs est sans limites. Longtemps, ils ont berné bon nombre d'entreprises en se faisant passer auprès de salariés de la direction financière pour leur supérieur hiérarchique et en leur intimant l'ordre de transférer de l'argent sur un compte fictif. Mais la manœuvre, dite «fraude au président», a fini par prendre une ampleur telle que les entreprises n'ont plus hésité à en parler, y compris aux médias. Conscients qu'ils risquaient d'avoir affaire à

ARTICLES LIÉS

FRAUDE
Des précautions à prendre aussi à l'export

ERREUR COMPTABLE DÉLIBÉRÉE
L'irrégularité comptable délibérée commise par un salarié n'empêche pas la société de demander le remboursement de l'excédent d'impôt payé

CASH MANAGEMENT
Le zéro papier, c'est pour bientôt !

RISQUE
Les tentatives de fraude se multiplient

des salariés plus méfiants, les escrocs ont aussitôt modifié leur approche.

Depuis quelque temps, ils s'attaquent ainsi aux fournisseurs des entreprises, en se faisant passer cette fois pour leur client. Les questions sont a priori anodines. *«La personne au téléphone prétexte vouloir faire le point sur ses dettes fournisseurs et demande incidemment quelle est la dernière facture à régler,* raconte le directeur financier EMEA de Louis Vuitton. *En fait, elle veut obtenir le numéro de facture et le montant dû exact pour rendre plus crédible la demande de virement sur son faux compte qu'elle adressera ensuite au groupe.»*

Bien que les entreprises soient désormais prévenues de la multiplication des risques de fraude, celles-ci continuent de prospérer. D'après une récente étude réalisée par la DFCG et Euler Hermes, 93 % des 150 directions financières interrogées en France ont été victimes d'au moins une tentative frauduleuse en 2015, contre 77 % l'année précédente.

«Une fois qu'ils ont récolté des informations sur une entreprise, les escrocs réitèrent systématiquement leurs tentatives de fraude, même après plusieurs échecs», **prévient Bernard Gall, trésorier adjoint d'Arianespace et président de la commission «Lutte contre la fraude financière» de l'Association française des trésoriers d'entreprise (AFTE).** Face à cette évolution, les directions financières doivent donc accroître leur vigilance, non seulement dans les PME, souvent en retard sur le sujet, mais aussi dans les grands groupes a priori plus avertis, mais où les risques, compte tenu de leur taille, sont démultipliés.

Instauration de bonnes pratiques

Parmi les premières précautions à prendre figure le suivi et le contrôle des virements. Il faut vérifier tout d'abord la structuration des coordonnées bancaires. *«Il y a peu de temps, une entreprise a décelé qu'une demande était frauduleuse en remarquant que les deux premières lettres de l'IBAN étaient l'indicateur de la Hongrie, alors que le fournisseur se situait en France»*, se rappelle Jean-Louis Di Giovanni, associé chez PwC au sein du département litiges et investigations.

Avec l'élaboration de nouvelles formes d'usurpation d'identité par les fraudeurs en vue d'obtenir un virement, une vérification supplémentaire s'impose. *«Dès qu'un changement de coordonnées bancaires est exigé, les directions financières doivent inciter leurs collaborateurs à demander systématiquement confirmation auprès du fournisseur, mais en veillant surtout à ne pas appeler le numéro figurant sur le courrier signalant le changement»*, recommande Jean-Louis Di Giovanni. **Si la demande de changement est effectuée par téléphone, la même prudence est de mise.** *«Il ne faut jamais utiliser la touche de rappel du téléphone,* alerte Bernard Gall. *Dans une récente affaire, un escroc était parvenu à faire afficher sur le téléphone d'une comptable, non pas son numéro d'appel, mais celui d'un fournisseur dont il avait usurpé l'identité !»*

La méfiance est d'autant plus de mise que les fraudes, élaborées de plus en plus à l'avance, visent désormais à modifier des informations généralement mal protégées.

«Dans un schéma évolué de fraude au fournisseur, les fraudeurs s'attaquent tout d'abord à des données jugées peu sensibles : les coordonnées postales ou téléphoniques du fournisseur, **explique Antoinette Gutierrez-Crespin, associée chez EY.** *Une fois que l'entreprise a intégré ces nouvelles coordonnées dans son système informatique, les fraudeurs reviennent à la charge en exigeant un changement de coordonnées bancaires. Même si l'entreprise se méfie de cette demande, il est trop tard, car elle s'adressera en cas de doute au contact frauduleux précédemment fourni.»*

Les fraudes sont toutefois loin de concerner uniquement les virements. Les directions financières sont aussi confrontées à la montée du risque cyber, ces attaques visant le réseau informatique de l'entreprise. Dans ce cadre, elles doivent impérativement sensibiliser leurs collaborateurs aux pièges que contiennent les courriers électroniques qu'ils reçoivent. *«Les fraudeurs envoient régulièrement des e-mails comportant des liens qui, si le destinataire clique*

dessus, téléchargent des logiciels malveillants, observe Jean-Louis Di Giovanni. *Ils peuvent alors crypter les données de l'ordinateur et exiger ensuite une rançon de quelques milliers d'euros pour rétablir l'accès aux données.»* **Les réflexes à adopter consistent alors à ne pas ouvrir les liens dont l'expéditeur est inconnu, mais aussi à réagir dès les premiers signes annonciateurs d'une cyberattaque.** *«Après avoir reçu un e-mail de la part du directeur financier, une trésorière s'est aperçue que ce dernier était en train de se faire pirater son ordinateur,* raconte Bernard Gall. *Comme il était en réunion, elle a immédiatement demandé au service informatique de détruire l'ordinateur du directeur financier pour éviter que la tentative de piratage ne réussisse.»* Les cyber-fraudeurs multipliant les approches pour endommager ainsi le système de l'entreprise, les collaborateurs doivent se montrer aussi vigilants pour tout matériel informatique susceptible de faire l'objet d'un usage malhonnête.

«Certains escrocs déposent intentionnellement une clé USB dans le parking d'une entreprise avec une étiquette indiquant "confidentiel" afin qu'un salarié soit tenté d'en lire le contenu, **rapporte Jean-Louis Di Giovanni.** *Dès lors que celui-ci l'insère dans son ordinateur professionnel, un logiciel malveillant peut pénétrer le système informatique et permettre d'en prendre le contrôle.»* La méfiance doit ainsi devenir le réflexe premier des collaborateurs, en toutes circonstances…

Une attention particulière doit enfin être portée aux salariés maniant des documents sensibles. Régulièrement, le directeur financier d'un groupe coté dans le secteur des services effectue ainsi le tour des bureaux pour vérifier qu'aucun document important, tel qu'une facture donnant le nom et les coordonnées des clients ou un RIB, n'est accessible à une personne extérieure à l'entreprise et insiste, le cas échéant, sur la nécessité de les ranger en lieu sûr.

Diffusion de l'information

En dehors de ces précautions, les salariés ne doivent pas hésiter à signaler toute situation anormale. Un réflexe d'autant plus important que les escrocs, sachant les entreprises plus averties, adaptent très rapidement leurs méthodes. *«Ils continuent à se faire passer pour le président, mais ils n'appellent plus directement le collaborateur, ils le préviennent par mail qu'il sera contacté par un avocat à propos d'un virement,* indique Bernard Gall. *Lorsqu'il reçoit l'appel en question, le collaborateur se montre ainsi peu méfiant car il s'attend à la demande que lui formule le faux avocat.»*

Mieux vaut donc prendre trop de précautions que pas assez. *«Dès qu'ils ont un doute sur le caractère anormal d'une demande, les salariés sont incités à prévenir l'audit interne, souligne le directeur financier d'un groupe industriel coté. Cette consigne est désormais bien intégrée puisque, lorsque j'ai récemment demandé à un responsable de filiale de payer des dividendes, celui-ci a d'abord contacté le siège pour s'assurer qu'il ne s'agissait pas d'une fraude !»* Les directions financières doivent d'ailleurs rassurer les salariés en leur garantissant qu'à aucun moment ce type de réflexe ne peut être sanctionné, car il s'agit souvent d'un argument employé par les fraudeurs pour faire céder leurs cibles.

Plus globalement, elles ont tout intérêt à largement communiquer autour du risque de fraude. *«Le groupe LVMH auquel nous appartenons remonte les cas de tentatives de fraudes financières subies par l'ensemble des entités, puis les diffuse tous les deux ou trois mois dans le cadre d'une note adressée à tous les responsables financiers du groupe, explique le directeur du contrôle interne et organisation de Louis Vuitton. A nous ensuite de sensibiliser nos équipes en nous appuyant sur ces exemples.»* Une pratique qui s'adresse aux collaborateurs du siège, mais aussi à ceux des filiales, y compris celles de petite taille situées à l'étranger. Souvent moins contrôlées que le siège ou les filiales plus importantes, elles sont en effet régulièrement prises pour cible par les fraudeurs et nécessitent donc de faire l'objet d'une attention accrue.

Le travail de sensibilisation passe alors par des sessions de formation, en ligne ou au cours de séminaires. Après avoir mis en évidence l'existence du risque, l'objectif de ces sessions consiste à identifier les réflexes à adopter selon la nature des soupçons.

«Nous nous appuyons sur des cas concrets pour former les équipes financières et comptables, **explique Olivier Rigaudy, directeur général adjoint finance chez Teleperformance**. *Nous*

montrons notamment comment de faux commissaires aux comptes réclament le solde des comptes des filiales au siège pour ensuite exiger auprès de ces dernières le règlement de leurs factures, ou comment de faux présidents prétextent un virement urgent pour une opération confidentielle. Nous attirons alors leur attention sur le caractère inhabituel de la demande, par exemple parce qu'elle concerne la Chine alors que la société n'a pas de relation financière avec ce pays, ou parce qu'elle comporte des fautes d'orthographe.»

Vérification de l'efficacité

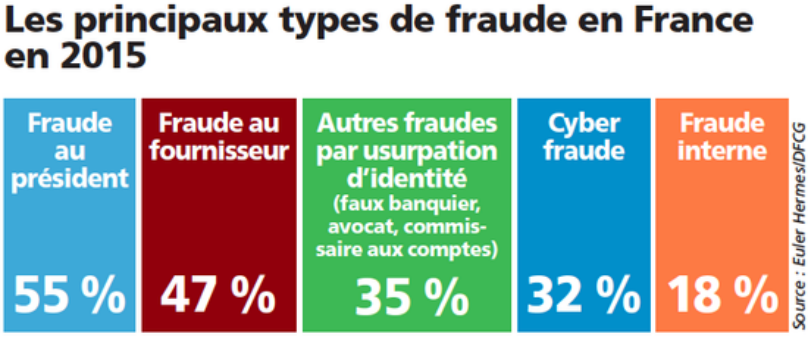
Ces formations ne suffisent toutefois pas en elles-mêmes. Il faut aussi vérifier qu'elles sont bien intégrées dans la gestion quotidienne de l'entreprise. Une précaution nécessitée par la rotation des équipes et l'évolution incessante des schémas frauduleux. A intervalle régulier, la direction financière d'un groupe dans le secteur des services prévient ainsi ses collaborateurs que, au cours des trois prochains mois, de fausses tentatives de fraude seront lancées. **Bilan : bien qu'étant prévenues, un nombre significatif de personnes réalise toujours des virements ou des changements de RIB sans vérification préalable.** *«Ce nombre diminue toutefois progressivement, à force de pédagogie»*, soupire le directeur financier.

Le dispositif préventif gagne à ce titre à être encore renforcé durant les périodes à haut risque. *«La veille des jours fériés et des vacances, nous procédons à un rappel des principes enseignés au cours des formations auprès des équipes financières et comptables»*, signale Olivier Rigaudy. Les escrocs profitent du fait que les responsables sont souvent remplacés par des professionnels moins expérimentés et que les virements ont de plus faibles chances d'être bloqués à temps.

Graduation des sanctions

Enfin, la dernière disposition à prendre pour lutter contre la fraude consiste à prévenir les salariés qu'ils risquent d'être sanctionnés s'ils n'appliquent pas les consignes de vigilance. *«Il n'est toutefois pas évident pour les entreprises de savoir comment traiter équitablement des salariés de bonne foi qui se sont laissé berner par des fraudeurs»*, reconnaît Antoinette Gutierrez-Crespin. En effet, déterminer quelle sera la sanction constitue un exercice délicat. **Si des sessions d'information ont déjà été assurées à maintes reprises, les directions financières se montrent généralement peu tolérantes.** *«Lorsqu'un salarié a fait preuve de négligence, notre réponse est proportionnelle aux conséquences de la fraude qu'il n'est pas parvenu à détecter,* indique Olivier Rigaudy. *Il est très rare qu'un tel comportement reste impuni.»* En général, lorsque la responsabilité du salarié a été prouvée, les sanctions peuvent aller de la simple mise à pied au licenciement.

En revanche, lorsque les collaborateurs se font tromper par un schéma de fraude encore mal connu, les sociétés font preuve de plus de clémence. Après avoir d'abord envisagé de licencier un salarié qui avait effectué un virement à un faux président alors que ce type de pratique était encore peu répandu, le directeur financier d'un groupe industriel coté a finalement décidé de ne pas le sanctionner, ayant pris conscience, après réflexion, qu'un tel scénario était difficile à anticiper. *«Les fraudeurs placent les collaborateurs dans des situations de tunnel psychologique, soit en les intimidant, soit en les mettant en confiance,* explique Michel Van Swieten, expert chez l'assureur fraude Euler Hermes France. *Nul ne sait quelle serait sa propre réaction en de telles circonstances.»* Une difficulté qui risque de persister au vu de la créativité des fraudeurs…



ATTENTION AUX RÉSEAUX SOCIAUX

- Pour sophistiquer leurs scénarios de fraude, les escrocs accumulent au préalable des informations qu'ils trouvent notamment sur les réseaux sociaux. *«Ils les utilisent de plus en plus pour se renseigner sur l'entreprise et ses collaborateurs,* prévient Jean-Louis Di Giovanni, associé chez PwC au sein du département litiges et investigations. *Les directeurs financiers doivent donc être attentifs à l'usage que font leurs collaborateurs des réseaux sociaux.»*

- Situation familiale, loisirs, dates de départ en vacances sont en effet autant d'éléments qui peuvent être utilisés à des desseins frauduleux. *«Je demande aux membres du comité exécutif et aux dirigeants financiers de ne pas être trop diserts sur Facebook ou LinkedIn quant aux informations en lien avec l'entreprise pour éviter que les escrocs ne s'en servent»*, indique Olivier Rigaudy, directeur général adjoint finance chez Teleperformance.

LA MISE EN PLACE D'UNE CELLULE DE LUTTE DÉDIÉE

- Face à l'accroissement du nombre de fraudes, de plus en plus de grandes entreprises mettent en place une structure dédiée à la lutte contre ce phénomène, comme ce groupe du CAC 40 qui, début 2015, a créé une cellule opérationnelle supervisée par le directeur financier, le directeur de l'audit et le directeur juridique. Composée de plusieurs collaborateurs (comptabilité fournisseurs, audit, achats, trésorerie, juridique), elle se réunit toutes les semaines afin de recenser les cas de tentatives de fraude au niveau du siège et des filiales.

- Outre ce dispositif préventif, les directions financières doivent également travailler à l'élaboration d'un plan à dérouler en cas de fraude avérée. *«Dès lors que le contrôle interne identifie un mouvement de fonds anormal, la direction financière est ainsi en mesure de réagir immédiatement»*, souligne Michel Van Swieten, expert fraude chez Euler Hermes France. Une réaction qui diffère selon le type d'escroquerie. *«En cas de fraude au virement, la direction financière doit en premier lieu contacter le banquier ainsi que la police ou la gendarmerie,* préconise Michel Van Swieten. *Elle a tout intérêt à avoir établi en amont les contacts et noté les numéros d'urgence à composer.*

À LIRE AUSSI

FRAUDE
Des précautions à prendre aussi à l'export

DROIT BOURSIER
L'AMF consulte sur les rachats de titres et les contrats de liquidité

ENTREPRISE
Comment se préparer à une perquisition fiscale

RÉFORME
La figure ambiguë des lanceurs d'alerte inquiète les auditeurs

ACTUALITÉS
DOSSIERS
ENTREPRISES & FINANCE
DROIT & AFFAIRES
ASSET MANAGEMENT
BLOGS & ANALYSES
COMMUNAUTÉS
PATRIMOINE

Menu

Newsletters
Événements
L'annuaire des Experts
Lettres professionnelles
S'abonner
Le magazine
Le groupe Option Finance

Services

SE CONNECTER À MON COMPTE

NOUS SUIVRE

Mentions Légales Conditions générales de vente Cookies Crédits Contact Plan du site