AVIS D'EXPERT

QUELLE REPONSE AUX NOUVELLES FORMES DE DELINQUANCE FINANCIERE ?

Dans un contexte de renforcement continu des obligations en matière de lutte contre la délinquance financière, les acteurs du secteur financier ont dû opérer un important changement de culture et mettre en place des dispositifs dédiés tout au long de la décennie qui vient de s'écouler.

Cependant, lutter contre la délinquance financière reste très éloigné du cœur de métier des acteurs concernés et leur degré de maturité apparaît très variable alors que la menace se fait de plus en plus pressante. En effet, cette menace évolue et s'adapte aux caractéristiques des domaines sur lesquels elle pèse. De même, elle appelle un changement d'état d'esprit et la mise en œuvre d'une réponse à la hauteur des enjeux.

Un contexte général facteur de risques et de transformations

En 2019, un rapport d'information de l'assemblée nationale sur l'évaluation de la lutte contre la délinquance financière en France soulignait la forte croissance des faits déclarés ainsi que « des pratiques frauduleuses de plus en plus sophistiquées et reposant largement sur le numérique »[1].

Depuis, la crise du COVID a joué un rôle d'accélérateur en matière de dématérialisation au sein des entreprises et a ainsi amplifié le mouvement déjà engagé par les délinquants en leur offrant encore plus d'opportunités. A cet égard, il convient d'insister sur le fait que l'automatisation des processus et la numérisation constituent non seulement des facteurs de risques mais influent également sur les caractéristiques des modes opératoires utilisés qui apparaissent de plus en plus sophistiqués et impersonnels. Tel un virus, la délinquance financière s'est adaptée aux principales caractéristiques des domaines sur lesquels elle fait peser sa menace.

[1] Rapport d'information sur l'évaluation de la lutte contre la délinquance financière déposé par le comité d'évaluation et de contrôle des politiques publiques et présenté MM. Ugo BERNALICIS et Jacques MAIRE Députés - 28 mars 2019

Le conflit Ukrainien a quant à lui entrainé un développement massif des attaques cyber créant ainsi un terreau propice au développement d'une cybercriminalité aux objectifs très variés allant de la pure malveillance au vol de données en passant par les ransomwares. A cet égard, il est important de souligner que la France est devenue l'un des pays les plus exposés aux ransomwares. Entre les fraudes et la cybercriminalité, 69% des entreprises ont été victimes d'une attaque en 2022, attaque qui atteint son objectif dans 25% des cas[2]. En quelques années, les risques ont décuplé et la cybercriminalité a ainsi engendré une véritable économie souterraine aux activités très diverses. Les données volées notamment en matière de santé pourront être revendues et servir à des groupes organisés, dans le cadre d'escroqueries massives dont les sommes détournées sont blanchies ou alimentent directement des activités criminelles ou encore terroristes.

Dès lors, on entrevoit que ces différentes formes de délinquance sont devenues complémentaires et s'intègrent désormais dans une véritable chaîne de valeur criminelle[3]. Le principal corolaire à ce constat est la nécessité pour les entreprises de faire évoluer leur approche des menaces et les réponses opérationnelles qu'elles leur apportent.

Une porosité entre les différentes formes de délinquance financière

Qu'il s'agisse du blanchiment de capitaux, du financement du terrorisme ou encore du respect des embargos et des sanctions internationales, les obligations qui pèsent sur les acteurs du secteur financier sont en constante évolution avec comme objectif principal le renforcement des dispositifs existants. Cette intensification doit d'abord permettre de répondre aux risques induits par les innovations technologiques dont les monnaies virtuelles sont un très bon exemple. De même, les dispositifs en place doivent prendre en compte la mondialisation des organisations terroristes et criminelles ainsi que leur redoutable capacité à s'adapter aux contre-mesures mises en place, à identifier et à exploiter les failles du système.

A cet égard, un élément de vulnérabilité des dispositifs -trop souvent mis en place afin de répondre à un besoin de conformité- réside dans le cloisonnement entre les différentes équipes qui sont confrontés en pratique à une seule et même délinquance.

Or, l'absence de dispositif intégré visant à décloisonner les structures ne permet pas de répondre efficacement aux différentes problématiques et manifestations de la délinquance financière dont les frontières s'estompent. Pourtant, traiter de blanchiment ou de financement du terrorisme au sein d'une entreprise d'assurances de bien et de responsabilité ou encore d'une mutuelle santé consiste en grande partie à lutter contre la fraude. Ce point n'est plus à démontrer mais force est de constater que les entreprises ayant mis en place une cellule unique dédiée à ces deux formes de délinquance restent très minoritaires.

Pareillement, la frontière entre fraude externe et fraude interne est devenue poreuse, comme le démontre la mise à jour régulière de fraudes dites mixtes. Ici encore, trop peu d'entreprises font le lien entre ces deux types de fraudes qui, mixées n'en constituent plus qu'un. A minima, ces fraudes mixtes requièrent une forte coordination entre les divers services de l'entreprise traitant généralement des deux types de fraude de manière isolée. En pratique, cette nécessaire coordination peine à se mettre en place tant sur le plan fonctionnel que sur le plan opérationnel au regard des réponses à apporter en cas de fraude avérée.

La cybercriminalité s'est quant à elle développée en quelques années pour devenir l'un des principaux risques pesant sur les entreprises tous secteurs confondus. Ici encore, il existe une importante porosité entre cette forme de délinquance et celle, plus classique, recouvrant des fraudes portant sur des flux financiers. L'analyse fine des cybermenaces permet ainsi de comprendre à quel point les activités criminelles sont devenues plus

[2] Baromètre Fraude 2022 réalisé par Euler Hermes et l'Association nationale des Directeurs Financiers et de Contrôle de Gestion (DFCG)
[3] L'article 2 de la directive (UE) 2018/1673 du 23 octobre 2018 visant à lutter contre le blanchiment de capitaux au moyen du droit pénal classe notamment comme activité criminelle la cybercriminalité, la fraude et la corruption.

complexes et interreliées car de plus en plus complémentaires. Si dans certains cas les cybercriminels poursuivent un but immédiat à savoir l'obtention de sommes sous la forme d'une rançon, certains d'entre eux se sont spécialisés dans le vol de données, pour les recycler dans le cadre de fraudes classiques. Ainsi, disposer du NIR et des identifiants d'un client d'une mutuelle permettra de commettre des escroqueries en toute impunité car il sera très complexe voire impossible de remonter aux auteurs des infractions.

On constate ainsi l'émergence de fraudes devenues impersonnelles dont la répression s'avère particulièrement délicate en pratique.

La cybercriminalité a donc contribué en quelques année au développement de toute une économie sur Internet fondée sur la fourniture de moyens pour commettre des fraudes et/ou dissimuler sa véritable identité.

Autrement dit, il est important que les organisations intègrent que lutter contre la cybercriminalité ne relève plus exclusivement d'un réflexe de défense mais participe également à la lutte contre la fraude.

L'adoption d'une approche holistique de la délinquance financière

La délinquance polymorphe et interconnectée qui s'attaque aux entreprises, notamment celles du secteur financier, se joue et profite opportunément des silos mis en place. S'il n'existe pas de contre mesure unique, il ne fait désormais plus aucun doute qu'il est nécessaire d'adopter une vision holistique des risques et les moyens systémiques afin de mieux les maîtriser.

Cette approche implique en pratique de faire évoluer les modèles organisationnels afin de garantir une gestion efficace du risque de fraude dans toutes ses dimensions et ce, tout au long de la chaine de valeur de l'entreprise. Elle doit s'inscrire dans une logique de coordination et implique une réelle agilité dans la capacité de l'organisation à s'adapter aux nouvelles formes de délinquances et aux modes opératoires émergeants. Cependant, cette approche reste actuellement peu développée car elle suppose au préalable une prise de conscience qui, en pratique fait souvent défaut.

Afin de faire évoluer les organisations et de créer de structures plus transverses à l'entreprise, il est donc nécessaire de réaliser un travail d'acculturation et d'appropriation autour des enjeux induits par l'évolution de la délinquance financière. Dans ce cadre, il faut tout d'abord arrêter de réduire le sujet à une question de conformité, avec en ligne de mire l'unique souci d'éviter des sanctions du régulateur. A cette fin, les entreprises doivent prendre de la hauteur en développant une véritable stratégie réglementaire fondée sur les intérêts communs que sous-tend la réglementation et en pensant au-delà de la lettre de la loi. Il convient ainsi de relever que l'engagement de l'organisation sur des sujets de lutte contre la délinquance financière s'inscrit également dans une logique qui va donc bien au-delà de l'unique respect de la réglementation.

Pour bâtir cette stratégie, il est nécessaire d'identifier et de mesurer les impacts organisationnels d'une approche globale au regard des risques auxquels l'entreprise est exposée.

Cela suppose d'établir une cartographie intégrant l'ensemble des risques de fraude qu'ils soient classiques ou découlant des nouvelles formes de délinquance. Dans ce cadre, il conviendra de s'attacher à identifier non seulement les risques mais aussi les acteurs impactés -directement ou indirectement- par leur gestion ainsi que les mesures et outils associés. Ce travail doit permettre la définition et le cadrage de la stratégie à adopter sur le court et moyen terme en fonction de l'effort à fournir dans le cadre d'une approche globale.

Une foi la stratégie arrêtée, il s'agira de bâtir le socle organisationnel qui a minima procédera notamment de la mise en place d'une gouvernance globale si l'adoption d'un dispositif opérationnel unique n'est pas retenue à court terme. Une gouvernance globale apparait centrale car elle permet de garantir la cohérence fonctionnelle, de pallier la rareté des

compétences en optimisant les ressources et d'organiser la mutualisation les outils de détection pour plus d'efficacité à moindre coût.

Au-delà des choix stratégiques de l'entreprise, il est important de souligner que mettre en œuvre une approche globale de la délinquance financière s'inscrit forcément dans le temps compte tenu de la nécessité de faire converger plusieurs dispositifs -souvent réglementaires- dans le cadre d'un plan d'action dédié. Ce plan devra être organisé autour du plier que constitue la stratégie retenue et impliquera un accompagnement au changement qu'il induit afin de créer du sens et donc de l'engagement au sein des équipes impactées. Ainsi, répondre aux défis que les nouvelles formes de délinquance financières imposent aux entreprises relève donc d'un véritable projet de transformation organisationnel et culturel.

Nul doute que les acteurs du secteur financier soient arrivés à la croisée des chemins. Ils peuvent continuer à subir et rester loin derrière les fraudeurs qui évoluent sans cesse ou bien agir et réagir en se mettant à l'état de l'art tout en investissant sur des activités à fort ROI.

CONTACTS

Quel que soit votre secteur d'activité, les équipes Talan Consulting spécialisées en matière de lutte contre la fraude et la délinquance financière vous accompagnent dans vos projets dont :

- *La définition d'une stratégie d'intégration et de la gouvernance associée*
- *Le re-engineering de processus LCF*
- *La mise en place de démarche de détection internalisée (Data / Pièces justificatives)*
- *L'optimisation des performances sur l'ensemble de la chaîne de valeur*

Frédéric Nguyen Kim

frederic.nguyen-kim@talan.com

Senior Advisor

Antoine Archambault

antoine.archambault@talan.com

Manager