MAI 2014

COMMENTARY

La lutte contre la cybercriminalité : un enjeu majeur pour les entreprises

La lutte contre la cybercriminalité constitue un enjeu juridique et économique considérable pour les entreprises. Le développement des nouvelles technologies et la révolution numérique n'ont fait qu'accentuer ce risque auquel les entreprises sont désormais confrontées. Plus encore, le montant des préjudices causés par des cyberattaques a explosé ces dernières années, pour atteindre un coût global de 750 milliards d'euros par an en Europe.

Par ailleurs, si les entreprises constituent de potentielles victimes de cette délinquance, elles n'en demeurent pas moins responsables de la sécurité de leurs propres données. Dès lors, seule une politique globale de cybersécurité permettrait de sensibiliser les Etats et les entreprises au phénomène des cybermenaces et d'y apporter une réponse non seulement technique mais également juridique. L'impératif de protection des données de l'individu et de l'entreprise devra figurer au cœur de cette politique.

L'émergence de la cybercriminalité

Une délinquance en plein essor. Si pendant un temps, la cybercriminalité fut l'œuvre d'individus isolés ou de petits groupes, on constate désormais qu'elle peut être le fruit d'organisations criminelles, souvent à dimension internationale. Le cybercrime s'est professionnalisé notamment avec la création de réseaux de plus en plus structurés, spécialisés dans le trafic de drogue, la prostitution, le blanchiment d'argent ou encore l'espionnage industriel.

La cybercriminalité est aujourd'hui l'une des formes de criminalité qui connaît la plus forte croissance tant au niveau national, qu'international. Les chiffres en la matière sont d'ailleurs particulièrement éloquents : en 2012, près d'une entreprise française sur deux déclarait avoir été victime d'attaques informatiques au cours des 12 derniers mois, contre 29 % en 2009. En outre, en se professionnalisant, la cybercriminalité est entrée dans une logique de rentabilité au profit du moindre effort : pour un investissement minimal, le préjudice subi peut s'avérer colossal. A titre d'exemple, les pertes liées au virus « I Love You » en l'an 2000 se sont élevées à plus de 4,7 milliards d'euros.

Une notion protéiforme recouvrant une grande variété d'infractions. Si aucune définition légale de la cybercriminalité n'est clairement établie, l'Organisation des Nations Unis a adopté une définition particulièrement large des actes de cybercriminalité comme étant *« tous faits illégaux commis au moyen d'un système, d'un réseau informatique ou en relation avec un système informatique »*. La cybercriminalité revêt de multiples formes que les grandes entreprises doivent appréhender en fonction de leur domaine d'activités.

Les principales infractions concernées sont les suivantes :

- les fraudes informatiques ou atteintes aux systèmes de traitement automatisé de données : accès ou maintien frauduleux, entrave au fonctionnement du système, introduction frauduleuse de données, falsification ou suppression frauduleuse de données ;
- les violations de données personnelles : traitement illégal de données à caractère personnel, collecte ou conservation de données à l'insu des personnes ou des entreprises, usurpation d'identité ;
- les atteintes à l'e-réputation des entreprises et la diffusion de contenus illicites : délits de diffamation et injure publique commis sur Internet ;
- la contrefaçon de marques, d'œuvres et de logiciels ;
- les infractions de droit commun commises via l'utilisation des nouvelles technologies, notamment par Internet : vol, abus de confiance, escroquerie.

Cette délinquance est ainsi diversifiée, complexe et très souvent internationale. Par ailleurs, la motivation des cyber-délinquants est particulièrement variée (gain financier, défi technique, défense d'une idéologie, espionnage industriel etc.). Plus grave encore, 80% des cyberattaques sont internes aux entreprises.

Une multiplicité de risques pour les entreprises. Les risques encourus par les entreprises en cas d'attaque cybercriminelle sont considérables. Une telle attaque a tout d'abord fréquemment d'importantes répercussions financières. Ainsi, l'arrêt - même temporaire - d'un service informatique a inévitablement pour conséquence un ralentissement de la production et peut entrainer des pertes d'exploitation substantielles pour l'entreprise. De même, la fuite de secrets industriels et la perte d'actifs incorporels stratégiques peuvent s'avérer gravement préjudiciables.

La cybercriminalité fait également peser un « risque de réputation » significatif sur les entreprises. En cas d'attaque, leurs données personnelles ainsi que celles de leurs partenaires commerciaux ou clients peuvent être dérobées et divulguées. L'impact peut ainsi s'avérer préjudiciable non seulement pour la réputation mais encore pour la crédibilité de l'entreprise auprès de ses partenaires.

Enfin, les entreprises doivent prendre conscience du risque pénal que la cybercriminalité leur fait courir, si notamment elles se trouvaient associées - via leur réseau informatique - à toute sorte d'actions illégales tel que le *spamming*, à savoir l'envoi massif et automatique, parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a récupéré les adresses électroniques de façon irrégulière. La responsabilité de l'entreprise pourrait également être engagée en cas de non-respect de la règlementation relative à la sécurisation des systèmes d'information.

Vers une strategie globale de « cybersécurité »

En matière de lutte contre la cybercriminalité, la coopération aux plans national et international n'a cessé de croitre au cours de ces dix dernières années. Si l'avènement de l'ère numérique a conduit à l'adoption de politiques nationales, la lutte contre les cybermenaces passe en effet incontestablement par des réponses coordonnées au niveau international.

L'existence de services spécialisés au niveau national. L'explosion du nombre des cyberattaques, a contraint la France à adopter une véritable politique de défense afin de protéger ses systèmes d'information. Elle s'est ainsi dotée de différents organes et services spécifiquement dédiés à la lutte contre la cybercriminalité au niveau de la police, de la gendarmerie ou encore des douanes, dont principalement :

- **l'Agence nationale de sécurité des systèmes d'information** (ANSSI), créée en juillet 2009 et chargée de proposer des règles en matière de protection des systèmes d'information de l'Etat. L'ANSSI assure également un service de veille et de détection des attaques informatiques et conseille les entreprises privées pour la sécurisation de leurs systèmes d'information ;
- **l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication** (OCLCTIC), chargé de lutter contre toutes les infractions liées aux nouvelles technologies de l'information et de la communication (piratage, usurpation d'identité, escroquerie etc.) et de coordonner au niveau national l'ensemble des actions de la police et de la gendarmerie ;
- **la Bridage d'enquêtes sur les fraudes aux technologiques de l'information** (BEFTI), qui intervient principalement sur des problématiques de propriété intellectuelle notamment en cas d'atteinte aux systèmes d'information (piratage, intrusion dans

les réseaux informatiques, contrefaçon de logiciels, fraudes téléphoniques etc.) et assiste les différents services enquêteurs sur des affaires de cybercriminalité ;

- **le Service technique de recherches judiciaires et documentation** (STRJD) qui a pour fonction de centraliser et exploiter les informations judiciaires qui lui sont transmises par l'ensemble des unités de la gendarmerie nationale notamment sur les infractions relatives à la transmission de données à caractère illicite sur Internet. Le service « Cyberdouane » a instauré quant à lui un dispositif de veille permettant de détecter et traquer les infractions commises sur Internet, notamment les actes de contrefaçon.

Si l'arsenal institutionnel s'est considérablement renforcé, il est essentiel de développer en parallèle l'arsenal judiciaire, en instituant une chaîne pénale spécialisée à compétence nationale pour réprimer les cyberattaques. A cet égard, les projets de création d'un pôle numérique à la Chancellerie dédié à la mise en œuvre de la politique pénale en matière de lutte contre la cybercriminalité et d'un poste de procureur européen sont tout à fait indispensables.

Une coopération européenne et internationale renforcée. Le cyberespace s'affranchit par nature de toutes les frontières étatiques. Ce caractère transnational impose aux Etats la mise en place d'actions concertées visant à établir des politiques de coopération européenne et internationale en matière de lutte contre la cybercriminalité. C'est dans ce cadre que la Directive 2013/40/UE relative aux attaques contre les systèmes d'information a été adoptée le 12 août 2013 par le Parlement européen et devra être transposée en droit interne avant le 4 septembre 2015. Elle vise à harmoniser les législations en vigueur en matière de lutte contre la cybercriminalité et à instaurer une coopération renforcée dans l'Union européenne par la mise en place d'un système coordonné de suivi des infractions.

La création du Centre Européen de Lutte contre la Cybercriminalité (EC3) en janvier 2013, dont l'objectif principal est la protection des entreprises européennes contre les activités illicites en ligne menées par des organisations criminelles et les attaques des systèmes d'information, a constitué le point d'orgue de cette coopération. Il centralise l'expertise et l'information, et apporte un soutien opérationnel dans le cadre d'enquêtes communes réalisées à l'échelle de l'Union européenne. En amont, ce centre prépare des rapports évaluant les risques de cybermenaces et publie, le cas échéant, des « alertes » précoces. L'EC3 met également à la disposition des unités répressives des États membres de l'Union européenne un service d'assistance (*« help desk »*) en cas de cyberattaques.

Enfin, une cellule de lutte contre la cybercriminalité au sein d'INTERPOL a également été mise en place afin de favoriser l'échange d'informations sur de potentielles cyberattaques, détecter les nouvelles menaces et communiquer aux pays membres les renseignements recueillis. Ce groupe apporte également son assistance dans le cadre d'enquêtes portant sur des cyberattaques.

Conclusion

Le cyber-risque constitue désormais une menace substantielle que les dirigeants d'entreprise doivent impérativement appréhender et anticiper. Une vigilance renforcée s'avère nécessaire à tous les échelons de la hiérarchie au sein des entreprises, garantes du respect du contrôle interne et de la protection de leurs actifs. Afin de préserver la confiance de leurs investisseurs et partenaires, les entreprises doivent en outre faire évoluer leur politique de sécurité informatique, dans le cadre d'une politique globale de cybersécurité.

Contacts

Bénédicte Graulle
Paris
+33.1.56.59.46.75
bgraulle@jonesday.com

Emmanuel G. Baud
Paris
+33.1.56.59.39.18
ebaud@jonesday.com