CYBER-SÉCURITÉ : VOTRE ENTREPRISE EST-ELLE BIEN ASSURÉE ?

Dans un rapport publié en 2019, l'assureur HISCOX souligne une augmentation très nette des entreprises ayant signalé avoir été la cible d'une cyber-attaque, de 45% en 2018 à 61% en 2019.

Ce constat ne risque malheureusement pas de s'améliorer cette année, puisque l'épidémie de Covid-19 a eu pour effet d'augmenter de manière très significative le nombre de cyber-attaques. C'est l'analyse faite par l'Orange Cyberdéfense, qui évalue entre 20 et 25% l'augmentation de ces incidents depuis le début de la crise sanitaire.

Le recours au télétravail est le facteur principal d'explication de la hausse constatée. En effet, les ordinateurs utilisés, les applications auxquelles les salariés ont recouru (au premier rang desquelles « Zoom » pour les entreprises qui n'étaient pas dotées d'un système interne de visioconférence) et plus encore les réseaux de connexion wifi au domicile constituent des points de vulnérabilité.

Les cyber-attaques sont de plus en plus sophistiquées (Logiciels malveillants, Ransomwares, Phishing, Attaque MTIM – Man In The Middle...) et présentent souvent les caractéristiques suivantes.

En premier lieu, on dit qu'elles sont invisibles, car la détection de l'incident peut être tardive. Ces incidents sont internationaux, tant dans leurs origines que dans leurs conséquences, le risque s'appliquant sur un réseau mondial et interconnecté. Enfin, les cyber-attaques sont incertaines, ce qui les rend donc assurables, même si l'aléa porte moins sur le « si » (« if ») que sur le « quand » (when).

L'ancien PDG de CISCO, John Chambers, déclare, pour illustrer la probabilité pour les entreprises de faire face à une cyber-attaque : « *Il y a deux types d'entreprises : celles qui ont été piratées, et celles qui ne savent pas encore qu'elles l'ont été* ».

Ces cyber-incidents ne concernent pas uniquement les grandes entreprises, les groupes industriels ou

Guillaume AKSIL

bancaires. Les TPE et PME sont de plus en plus ciblés, en raison notamment des mesures de sécurité informatique en place dans ces entreprises, qui peuvent être insuffisantes.

La digitalisation croissante des activités et la généralisation du télétravail sont des facteurs ayant pour effet d'accroître la sensibilité des entreprises aux cyber-attaques.

Quelles sont les conséquences pour une entreprise, victime d'un cyber-incident ? Puis-je m'assurer contre ce type de risques et quelles sont les garanties auxquelles je peux prétendre ?

LA GESTION D'UNE CYBER-ATTAQUE : UN ENJEU FINANCIER ET RÉPUTATIONNEL

Chaque année, le nombre d'entreprises déclarant être victimes d'une cyber-attaque augmente.

Certaines conscientes de ce nouveau risque investissent massivement dans la sécurisation de leurs infrastructures informatiques. D'autres, pour lesquelles la menace étant moins précise, moins connue, sont moins bien préparées.

Il existe actuellement de grandes disparités dans le niveau des capacités de gestion du risque cyber. Pourtant, les attaques sont plus fréquentes et plus coûteuses, au regard de leurs conséquences.

Pour illustrer nos propos, nous prendrons deux exemples pratiques, afin de mieux mesurer les incidences d'une cyber-attaque sur l'activité d'une entreprise.

Une entreprise exploite un site d'e-commerce. Des pirates informatiques parviennent à infiltrer son système informatique et dérobent des millions de données personnelles sur ses clients, parmi lesquels leurs numéros de cartes bancaires.

Dans cette hypothèse, l'entreprise pourrait être contrainte de bloquer momentanément l'accès à sa plateforme, entraînant ainsi une perte de chiffre d'affaires. Elle devra engager des frais pour reconstituer ses données et également informer la CNIL, et le cas échéant, ses clients du vol des informations les concernant, et ce, afin de respecter ses obligations réglementaires résultant du Règlement Général sur la Protection des Données Personnelles (RGPD).

Outre les coûts nécessaires à la reprise de l'activité, cette cyber-attaque peut entraîner une perte de confiance des clients et nuire à la réputation de la société et à l'image de sa marque.

Une entreprise du secteur de l'industrie agroalimentaire, dont les chaînes de production sont entièrement informatisées, est victime d'une cyber-attaque. En cas d'incident de cette nature, sa production pourrait être interrompue provoquant des pertes d'exploitation consécutives à cet évènement. Elle pourrait même perdre une partie de ses clients finaux, si elle n'est pas en mesure de redémarrer rapidement son activité.

Ce dernier exemple est un scénario malheureusement réaliste. Norsk Hydro et Saint-Gobain, des fabricants de matériaux de premier plan, ont été victimes de cyber-attaques, qui ont eu pour effet de désorganiser leurs capacités de production pendant plusieurs semaines.

COMBIEN COÛTE UNE CYBER-ATTAQUE ?

Pour le cas de Saint-Gobain, la cyberattaque NotPetya, qui a provoqué une indisponibilité du système d'information du groupe, a coûté pas moins de 80 millions d'euros de résultats[1].

1 - https://www.argusdelassurance.com/gestion-des-risques/grands-risques/saint-gobain-la-cyberattaque-notpetya-lui-a-coute-80-m-de-resultats-amrae-2018.126604

Selon une étude réalisée auprès de grandes entreprises par le cabinet Accenture, le coût moyen d'une cyber-attaque pour une société française de grande taille a augmenté de 23% en un an, et est évalué à 8,6 millions d'euros en 2019[2].

Hiscox, assureur spécialisé dans la couverture des risques cyber, a publié en 2019 un rapport confirmant l'augmentation des pertes financières liées aux cyber-incidents[3].

Si les grandes entreprises sont particulièrement ciblées et supportent une part importante des coûts cumulés des sinistres survenus, **la cybercriminalité coûterait, en France, 700 millions d'euros par an aux PME**, selon une enquête réalisée par l'IRT SystemX.

Ce chiffre doit être mis en perspective avec le montant des primes mondiales collectées sur le marché de la cyber-assurance, qui était évalué à 3,5 milliards de dollars en 2016. À cette même époque, le marché américain représentait à lui seul 85 à 90% de ces primes et la France environ 40 millions d'euros (soit ≈ 1,1%).

Un chiffre dérisoire lorsqu'on le rapporte au coût total des sinistres consécutifs à une cyber-attaque !

Il est vrai que les États-Unis ont pris de l'avance, s'agissant de l'offre d'assurance cyber, puisque les premiers contrats cyber « purs » sont apparus dès le début des années 2000.

De nombreux observateurs prédisaient un doublement du volume mondial des primes de cyber-assurance d'ici à 2020. Nous ne sommes pas en mesure de confirmer l'évolution de ce marché, mais gageons que les souscriptions se sont accélérées ces trois dernières années. Cela est en tout cas souhaitable.

Aujourd'hui, plus de la moitié des très grandes entreprises disposent d'une couverture d'assurance contre les risques cyber. À l'inverse, les TPE et les PME souscrivent assez peu ce type de garanties, alors qu'elles ne sont pas moins exposées à ces risques.

Comment expliquer cette différence observée entre les pratiques en vigueur au sein des très grandes entreprises et celles des TPE/PME ?

D'une part, les TPE/PME comptent rarement au sein de leurs effectifs des experts de la cyber-sécurité, qui pourraient les sensibiliser sur les mesures de sécurité à mettre en œuvre.

D'autre part, ces entreprises n'ont pas conscience des risques encourus et de leur exposition, s'estimant au contraire à l'abri de ce type de menaces, notamment lorsque leur activité n'est pas directement liée au numérique. Elles ignorent également l'existence de contrats d'assurance couvrant les risques cyber.

LE RECOURS À LA CYBER-ASSURANCE : LA SOLUTION POUR MINIMISER LES RISQUES ENCOURUS

Nous ne reviendrons pas ici sur le débat de l'assurabilité des cyber-risques, qui nous paraît aujourd'hui dépassé, du seul fait de l'existence sur le marché de contrats d'assurance couvrant ce type de risques.

Face aux conséquences d'une cyber-attaque, la souscription d'une cyber-assurance est intéressante.

En tant qu'avocat en droit des assurances, nous accompagnons nos clients pour étudier leurs polices d'assurance actuelles et clarifier ainsi les garanties dont ils disposent et celles qu'ils devraient souscrire pour se prémunir contre le risque cyber.

Cette phase d'audit préalable est cruciale, puisque de nombreux contrats « traditionnels » de dommages et de RC couvrent le risque cyber, à défaut de l'avoir expressément exclu. On retrouve ici la problématique des **garanties silencieuses**, qui n'est pas sans rappeler le débat actuel autour de la prise en charge par les assureurs des pertes d'exploitation, dans le cas d'une épidémie.

En novembre 2019, l'ACPR a d'ailleurs publié une note appelant les assureurs à clarifier l'étendue et l'articulation des couvertures d'assurance cyber.

Actuellement, il existe deux types de couvertures des cyber-risques.

D'une part, les garanties qualifiées d'« implicites » par l'ACPR. Ce terme recouvre l'hypothèse dans laquelle l'entreprise est bénéficiaire d'un contrat d'assurance Multirisque professionnel, d'une police Dommages aux Biens ou « Tous Risques Sauf », qui n'exclut pas expressément les dommages consécutifs à une cyber-attaque.

Rappelons ici que le Code des assurances impose que les exclusions prévues dans les polices soient formelles, limitées (article L. 113-1 du Code des Assurances) et rédigées en caractères très apparents (article L. 112-4 du Code des Assurances). En d'autres termes, tous les évènements qui ne sont pas expressément exclus sont susceptibles d'être pris en charge.

Ces garanties « implicites » sont extrêmement risquées pour les assureurs, lesquels n'ont pas voulu couvrir le risque. Il peut s'agir d'une erreur rédactionnelle ou encore du cas d'anciennes polices souscrites à une époque où le risque informatique n'était pas aussi présent et qui survivent par le jeu de la tacite reconduction. Les assureurs, n'ayant pas entendu garantir le risque cyber, n'ont pas pris soin de le prendre en compte dans la détermination du montant des primes. Cela n'est pas sans poser de difficultés au niveau actuariel, les risques cyber n'ayant pas été anticipés parmi les évènements assurables.

Les contrats de dommages aux biens n'excluant pas expressément le risque cyber sont susceptibles d'être mis en œuvre, lorsque la cyber-attaque cause des dommages matériels et des dommages immatériels consécutifs. Concrètement, prenons l'exemple de l'incendie d'une centrale nucléaire causé par une attaque informatique. L'usine atteinte par l'incendie peut être partiellement détruite. L'entreprise exploitante du site fera donc face à des dommages matériels, qui pourront être pris en charge par son assurance dommages.

Ce cas de figure n'est pas fictif, mais correspond à un scénario réel qui s'est déroulé en Arabie Saoudite. En effet, le système informatique d'une raffinerie de pétrole a été piraté à l'aide d'un virus de type « Stuxnet », qui a provoqué l'incendie et l'explosion de l'infrastructure.

Il convient d'insister sur le fait que seuls les dommages matériels et immatériels consécutifs peuvent être pris en charge. À l'inverse, les dommages immatériels non consécutifs ne peuvent être couverts.

2 - https://www.accenture.com/fr-fr/insights/security/etude-cout-du-cybercrime
3 - https://www.hiscox.fr/courtage/sites/courtage/files/documents/rapport_hiscox_gestion_cyber_risques.pdf