LES FONDAMENTAUX

ASSURANCES DE DOMMAGES

L'ASSURANCE DES LIGNES FINANCIÈRES

Responsabilité des dirigeants et mandataires sociaux,
Rapports sociaux,
Fraude et détournements,
Risques cyber

Dominique Bercovici

L'ARGUS de l'assurance ÉDITIONS

Sommaire

Ils édictent des réglementations pour protéger leurs citoyens (cf. directives RGPD et NIS), et mettent en place des défenses pour faire face aux attaques de leurs pairs, dans un cyber-espace où chacun doit savoir attaquer pour se défendre.

A – Cyber guerre et cyber terrorisme

L'environnement hostile ne se limite pas aux cyber-criminels. Il est d'ailleurs difficile de faire la part, dans nombre d'attaques cyber, de qui les instrumentalise, en tire profit et qui se cache réellement derrière, quand elles sont revendiquées ou attribuées.

On constate d'ailleurs que les attaques ciblées font de plus en plus de victimes collatérales, pour masquer leur véritable cible, ou arriver jusqu'à elle.

Les attaques à visée politique ratissent pour leur part généralement très larges, et font nombre de victimes par ricochet, pour atteindre les maillons faibles à l'intérieur de groupes de sociétés.

B – Les lois extraterritoriales

Les États censés être des alliés indéfectibles, ne manquent pas non plus de défendre leurs intérêts de manière agressive, par l'édiction de lois à portée extraterritoriale (cf. les « Patriot Act » et « Cloud Act » américains).

Des mesures de protection, qui peuvent être perçues par certains États (les États-Unis en l'occurrence) comme des mesures discriminatoires ou de rétorsion, sont prises, par l'Union européenne ou des États, afin de faire respecter les droits de leurs propres citoyens. Il s'agit notamment d'instaurer des dispositifs de protection minimale (Safe harbor et Privacy shield), pour leurs citoyens dont les données sont exportées sans leur consentement à l'étranger. Ces dispositifs n'ont toutefois pas été jugés suffisants pour la Cour de justice de l'Union européenne (cf. arrêt CJUE du 17 juill. 2020 « Schrems II »).

C – Les libertés individuelles

Si les réglementations protectrices mises en œuvre par les législateurs fédéraux aux États-Unis ou par l'Union européenne, ne cherchent pas à entraver le développement de l'économie numérique, elles instaurent des dispositifs de consentement, de sécurisation des données, mais également de protection des droits de la personne. En effet, ces mesures visent à imposer aux acteurs du numérique, des limites à respecter, par des lois dites de « Privacy » et de « Data breach », comme le Règlement Général de Protection des Données (RGPD) du 27 avril 2016, sous menace d'imposantes sanctions administratives supposées être dissuasives.

Section II – Les Risques

Avec la place prépondérante prise par les systèmes d'information et de traitement des données dans l'exercice des activités des entreprises, de nouvelles vulnérabilités et des contraintes fortes ont émergé, auxquelles l'entreprise doit faire face.

On constate ainsi :

- le ciblage direct ou indirect de l'entreprise par des attaques informatiques de plus en plus fréquentes et sophistiquées ;

- la grande dépendance des activités de l'entreprise au bon fonctionnement et à la sécurité de ses systèmes d'information, ainsi qu'aux prestations externalisées des sociétés de services informatiques ;
- le rôle clé des données, de toute nature, pour l'exercice des activités et la réussite du modèle économique de l'entreprise ;
- le rôle grandissant de l'État, garant à la fois de la liberté d'exercice des activités numériques, de la sécurité des réseaux mais aussi, de la protection des libertés individuelles.

I – Les systèmes d'information

Les systèmes d'information et les données sont désormais au centre de l'activité des entreprises. Leur indisponibilité, leur interruption ou leurs dysfonctionnements fragiliseraient sérieusement l'entreprise.

La survenance d'un incident de sécurité a de multiples causes que l'entreprise doit prévenir ou sécuriser. Elle emporte de multiples conséquences auxquelles les directions informatiques et de la sécurité des systèmes d'information doivent remédier, faute d'avoir été en situation de les prévenir.

Tout commence par la sécurité. Cet ouvrage n'a pas pour objet de décrire les moyens, outils, méthodes et pratiques auxquels les experts en la matière font appel, ni d'en identifier les limites et les impasses. Des réponses sont apportées sur ce sujet par l'ouvrage « Risques techniques, audit et assurance » de Denis Legrand, Franck Le Maine et Patrick Thourot, édité dans cette même collection des « Fondamentaux de l'assurance - Dommages ». Nous nous contenterons de relever quelques éléments des politiques de cyber-sécurité qui peuvent illustrer notre propos.

La sécurité informatique doit assurer la disponibilité, l'intégrité et la confidentialité des systèmes d'information et des données.

La disponibilité renvoie au caractère opérationnel et à l'exigence de continuité du service des systèmes d'information. Elle requiert une politique de protection des systèmes d'information et de sauvegarde des données.

L'intégrité des ressources peut être garantie, notamment lorsque les équipes informatiques peuvent s'assurer que les données n'ont pas été modifiées à l'occasion d'une intrusion malveillante dans les systèmes d'information.

La confidentialité des données est assurée par la politique de contrôle des accès et par les mesures de chiffrement.

La sécurité informatique se déploie au niveau de la sécurité physique des équipements, de la sécurité logique des logiciels, des applications et des données, de la sécurité de l'exploitation et des réseaux de transmission et de communication.

La cyber sécurité doit garantir la maîtrise des risques crées par l'exploitation des systèmes d'information.

Les mondes de la cyber-sécurité et de l'assurance se retrouvent autour des notions d'analyse et de gestion de risques, appréhendées, pour ce qui concerne l'assurance sous le prisme, limité, mais à la mesure des solutions à notre disposition, des risques transférables sur un contrat d'assurance dédié aux risques cyber.

A – Les causes de l'incident cyber

Divers facteurs peuvent déclencher un incident de sécurité cyber, sur lesquels la politique de cyber-sécurité a des moyens d'agir et l'assurance cyber peut apporter des solutions.

1° Les facteurs humains

Dans ce monde où les travaux d'exécution, les traitements et même l'intelligence, sont confiés aux machines, aux programmes et autres algorithmes, le facteur humain reste une cause majeure à l'origine des incidents de sécurité.

L'homme, qui n'a pas la prétention qu'ont parfois les prophètes du nouveau monde cybernétique et numérisé, d'être sans défaut, a été de tout temps, dans les travaux qui le mobilisent, parfois contre son gré, guidé par l'avidité, la distraction et la paresse. Pour être moins négatif, on peut y ajouter l'insuffisance d'information.

Ces faiblesses sont susceptibles de marquer tout le process d'utilisation de l'information, depuis la conception des logiciels, le pilotage de la gouvernance, la mise en œuvre des mesures de prévention, de surveillance et de remédiation.

a) Malveillance informatique

L'importance majeure des systèmes d'information dans l'activité des entreprises a été perçue par les personnes avides de profit rapide et sans grand risque physique et même juridique.

La malveillance de l'homme exploite les failles matérielles et logicielles des systèmes d'information, qui ont pour origine les erreurs et omissions d'autres hommes, et vient ainsi perturber le monde harmonieux « seamless », des réseaux connectés.

Elle peut également provenir de complicités à l'intérieur du système.

Le virus informatique et le malware sont les instruments privilégiés des opérateurs malveillants, qu'il s'agisse de bandes criminelles, de hackers joueurs ou d'« hactivistes », idéalistes et/ou politisés, ou de toute autre initiateur qui ne tient pas à dévoiler ses intentions.

Le logiciel malveillant permet le sabotage, l'espionnage, la fraude, afin de saisir toute opportunité immédiate ou, de programmer à un moment propice le logiciel malveillant, et atteindre ainsi l'objectif recherché.

- **Failles de sécurité**

Il s'agit notamment d'exploiter, les failles de sécurité laissées par l'humain, qu'il s'agisse du concepteur d'un système d'exploitation, du programmeur système d'exploitation ou d'un d'un logiciel externe, de l'acte d'un collaborateur du département informatique, d'un prestataire de l'entreprise, ou d'un utilisateur négligent.

Il peut également s'agir du non-respect de règles de sécurité informatique d'un collaborateur de la Direction des Systèmes d'Information (DSI) ou d'une simple négligence d'un employé, trompé par un email compromis, par exemple.

- **Prise de contrôle du système d'information**

Les acteurs de la cyber-criminalité peuvent prendre le contrôle d'un système d'information en affichant leurs exigences, par l'insertion d'un rançongiciel dans le système d'information, ou en activant un logiciel malveillant qu'ils y ont introduit.

- **Cyber-terrorisme, cyber-guerre, sabotage**

Les motivations des acteurs de la cyber-malveillance se sont diversifiées.

Il s'agit désormais d'affaiblir une entreprise concurrente, de menacer ou de surveiller un État ennemi, mais également allié, de saboter ses projets, lorsqu'ils vous déplaisent (cf. le malware « Stuxnet » destiné à saboter des centrifugeuses du programme nucléaire iranien embarqué dans des composants de biens d'équipement).

Ainsi, à côté de menaces réelles et parfois systémiques contre les réseaux de pays entiers (cf. les attaques contre les réseaux informatiques de l'Estonie et de l'Ukraine) se retrouvent victimes par ricochet ou en tant que cheval de Troie, des entreprises totalement étrangères à l'intention de leur initiateur.

- **Espionnage**

L'espionnage économique et le vol ou la copie de travaux de recherche, ou d'actifs immatériels de toute nature (base de données, études de marché, plans stratégiques, secrets d'affaires, etc.), sont désormais des objectifs, sous-traités aux bandes criminelles, par des donneurs d'ordre (entreprises ou États concurrents), qui préfèrent rester discrets, en rémunérant ces opérateurs pour leur savoir-faire en matière d'intrusion et de vol de données.

b) Erreur informatique

L'erreur, la faute ou l'omission sont humaines. Des collaborateurs de l'entreprise peuvent faciliter l'intrusion de tiers malveillants, comme complices, mais également de manière tout à fait innocente, sans intention de nuire, faute d'un comportement averti.

L'erreur peut également relever de l'incompétence du collaborateur, d'insuffisances professionnelles, d'un défaut de commandement ou de l'incapacité des équipes à faire face à un événement imprévu et irrésistible, telle une attaque cyber malveillante.

Elle peut enfin résulter de l'indisponibilité du personnel, en nombre suffisant, notamment à un moment clé ou pour remédier à un problème.

2° Les facteurs technologiques

Les systèmes d'information ont eux-mêmes leurs faiblesses intrinsèques, de conception ou de fonctionnement en réseau.

a) Destruction et dysfonctionnements des systèmes d'information

Divers incidents peuvent rendre les équipements informatiques indisponibles ou dysfonctionnels, tels que :

- l'indisponibilité suite à une attaque informatique, comme celle causée par le ransomware « Not Petya », sur les serveurs et PC d'entreprises, rendus provisoirement ou définitivement inutilisables ;
- la panne et le dysfonctionnement interne de l'équipement informatique ou du support ;
- les dommages aux installations informatiques par incendie et événement naturel.

b) Logiciel

Les problématiques tiennent à l'erreur de programmation, de configuration et de codage qui ne permettent pas l'obtention des résultats attendus en matière de connexion, de traitement des données, ou qui se manifestent par un « bug » dont l'origine est difficile à retracer, et pour lequel la remédiation peut prendre beaucoup de temps.

Lorsqu'il s'agit de logiciels antivirus, ils peuvent également manquer à leur objet, si le virus est un « zéro day ».

c) Intégration des systèmes

Le sujet est souvent assez peu pris en considération, car comme pour le « bug », on n'en voit que les conséquences dommageables, sans en identifier les causes, qui sont souvent multiples et, par nature, sans lien entre elles.

Elle tient souvent à des problèmes de conception, d'articulation et d'intégration des systèmes entre eux. Il ne s'agit pas d'erreurs individuelles, mais le résultat de trop de complexité, et d'un manque de directives, de coordination ou d'intégration ; chaque partie fonctionnant par elle-même et pour elle-même, mais l'ensemble dysfonctionnant, voire ne répondant pas.

3° Les facteurs de dépendance

L'informatisation et la numérisation des entreprises induisent des dépendances à des prestataires et à des fournisseurs de matériels, de logiciels ou de prestations de services informatiques.

L'entreprise doit s'assurer non seulement de la qualité et de la disponibilité des produits et des services qui lui sont nécessaires, mais également de la sécurisation des réseaux, des systèmes d'information et des données. En effet, lorsque cette sécurisation n'est plus assurée, cela peut d'une part, contaminer les systèmes d'information et les données de l'entreprise et d'autre part, la conduire à interrompre ses activités informatiques.

a) Prestataires d'utilités

Les fournisseurs d'utilités, à savoir les distributeurs d'électricité, les entreprises de télécommunication et les fournisseurs de services internet, sont eux-mêmes exposés à des menaces très importantes.

L'interruption ou la perturbation de leurs activités peut résulter d'une menace ou d'une attaque malveillante, qu'elle soit directe et ciblée, ou indirecte, afin d'atteindre d'autres cibles connues des seuls initiateurs de l'attaque (cf. attaques informatiques contre serveurs DNS rendant indisponibles les adresses IP).

Eu égard à leur rôle central dans le fonctionnement et la connexion des réseaux, tout dysfonctionnement, toute attaque qui les menace ou les atteint, et de manière plus générale, tout incident de sécurité, fait nécessairement un grand nombre de victimes collatérales.

Le risque présente de fait, un caractère systémique pour l'ensemble des entreprises servies par ces fournisseurs (« black-out »).

b) Prestations de services informatiques

L'entreprise est censée avoir plus de prise sur certaines prestations de services informatiques, étant en mesure de faire jouer la concurrence et d'associer les compétences propres de ses équipes informatiques en matière de cyber sécurité à celles spécialisées de ses prestataires.

La dépendance varie selon le type de prestations.

Elle est forte en matière de systèmes d'exploitation, de progiciels et de logiciels, qu'il s'agisse d'organisation (ERP), de commerciaux (CRM) ou de process, où certains fournisseurs globaux sont en position dominante.

En matière de prestations informatiques externalisées, maintenance (applicative ou en condition opérationnelle), hébergement, paiement ou encore services cloud, l'entreprise a la possibilité de définir la portée ainsi que le cadre de l'externalisation et de coopérer avec le prestataire.

On doit prendre en compte les grandes difficultés des entreprises à négocier ou à accéder aux programmes de cyber sécurité des prestataires de services informatiques à présence globale.

Ces derniers revendiquent en effet, pour leur part, leurs capacités d'investissement et de déploiement incomparables en la matière, pour garantir, disent-ils, une sécurisation maximale de leurs prestations, sous plafond de responsabilité et engagements en « Service Level Agreement » (SLA), limités toutefois.

Il faut noter que le RGPD, nous le verrons ultérieurement, organise le contrôle de la sécurisation des données traitées par les sous-traitants (« data processor »).

c) Prestataires divers

Insérée dans un monde global, l'entreprise est vulnérable aux risques cyber auxquels sont exposés ses fournisseurs et prestataires de services, en amont comme en aval de sa production et de sa distribution.

On a pu constater, dans l'actualité récente, des sinistres cyber qui ont eu un impact significatif sur les clients de fournisseurs et prestataires non informatiques.

En matière de logistique, on peut citer les attaques cyber contre l'entreprise de messagerie « Fedex/ TNT Express » qui a coûté 300 millions de dollars de pertes d'exploitation à l'entreprise et contre l'entreprise de transport maritime danoise « Maersk », touchée pour un montant estimé équivalent. Dans les deux cas, les pertes en résultant subies par leurs clients non livrés n'ont pu être évaluées.

En matière de marketing, l'affaire « Cambridge Analytica », très médiatisée, parce qu'impliquant Facebook, démontre le risque auquel la divulgation non autorisée de données personnelles hébergées par un tiers, peut exposer une entreprise, à l'égard de ses clients et eu égard à sa réputation.

d) Conditions économiques et juridiques

L'externalisation des prestations s'accompagne le plus souvent de clauses limitatives de responsabilité imposées par le fournisseur ou le prestataire de services, que celui-ci ait la capacité de les imposer ou qu'elles relèvent des clauses habituelles de la profession ; l'indemnisation est généralement équivalente au montant de la somme perçue pour la prestation.

Ces pratiques tendent en fait, à faire supporter à l'entreprise, donneur d'ordre, l'essentiel des risques financiers afférents à l'interruption ou à la perturbation des services informatiques qu'elle attendait, en lieu et place de ce dernier.

4° Les facteurs d'organisation

Les risques proviennent également de l'intérieur de l'organisation de l'entreprise.

Les entreprises, qui dépensent des millions d'euros, sur des solutions technologiques, doivent également se préoccuper d'accorder les ressources humaines et financières, définir les politiques et les procédures nécessaires, pour faire en sorte que ces technologies fonctionnent et ne soient pas une source de vulnérabilité.

a) Défaillance de la prévention et de la sécurisation

Dans le cadre du management de ses risques et du déploiement de ses politiques de cyber sécurité, l'entreprise doit gouverner la sécurité informatique en prenant les mesures de sécurité, techniques et organisationnelles que prévoient, dans l'Union européenne, le RGPD et la directive « Network and Information Security » NIS, ainsi que les textes des lois fédérales ou des États fédérés des États-Unis en matière de « data breach » (cf. infra).

Leurs insuffisances et défaillances à atteindre les objectifs recherchés à raison d'un manquement dans la conception ou dans l'exécution, peuvent avoir des conséquences négatives pour l'entreprise, notamment au niveau des alertes et des procédures d'« escalation », qui sont supposées, en permettant une remédiation plus rapide, limiter l'impact d'un incident de sécurité et y mettre fin plus rapidement, sans que l'entreprise n'ait à subir d'interruption ou de perturbation de services dommageable.

b) Défaillance de la conformité

La cyber sécurité s'insère dans une culture de la sécurité qui doit être diffusée à tous les niveaux de l'entreprise, en suivant en particulier, les principes d'hygiène informatique.

Les mesures organisationnelles incluent la mise en place d'un référentiel de sécurité qui facilite la réalisation opérationnelle de la sécurité informatique.

Les mesures d'évaluation des politiques de cyber sécurité et de contrôle s'inscrivent dans le respect des règles de conformité ou de « compliance ». Elles décrivent les process d'organisation, d'audit et de contrôle, internes ou externes à appliquer aux systèmes d'information, à tout le moins, dans les grandes entreprises.

L'inadéquation des mesures mises en place, affaiblit l'entreprise et peut l'exposer à des sanctions.

Sur un plan qui peut être perçu comme anecdotique, le télétravail dans le cadre de la crise du Covid 19, source de vulnérabilité concrète pour les entreprises, par le nombre de sources individuelles d'intrusion dans les systèmes d'information de l'entreprise, rappelle l'importance de la sensibilisation des collaborateurs aux risques qu'ils peuvent causer ou éviter par leur attention et leur discipline.

c) Risques juridiques

Comme nous le verrons plus loin, le renforcement des législations sur les risques informatiques et numériques, expose l'entreprise à des procédures réglementaires visant à la remédiation comme à la sanction des comportements non conformes (cf. RGPD), ainsi qu'à la réparation des préjudices subis par les victimes de ces défaillances.

B – Les conséquences de l'incident cyber

La cyber-sécurité a comme ambition de réduire le risque à un niveau acceptable. L'assurance est sur la même ligne, puisqu'elle considère ne pas avoir vocation à accepter des risques que l'entreprise est en mesure d'éliminer elle-même ou, à défaut, de supporter sur ses propres fonds, moyennant un certain niveau d'auto-assurance.

Sous cette promesse, nous chercherons à identifier ci-après les conséquences financières de différents scénarios de sinistres.

1° Risques pertes propres – « First Party »

a) Interruption et perturbation de l'activité

La première conséquence d'un incident de sécurité, qu'il soit d'origine malveillante ou accidentelle, est l'indisponibilité du système d'information de l'entreprise ou de son prestataire d'externalisation.

Il peut en résulter des pertes d'exploitation subie par l'entreprise, à laquelle celle-ci doit remédier, afin d'y mettre fin ou d'en limiter les effets.

Les activités interrompues, partiellement ou totalement, perturbées, ralenties ou fonctionnant en mode dégradé, peuvent concerner différents domaines d'activités de l'entreprise.

Il peut s'agir :

- d'activités de production, de données d'exploitation compromises, etc. ;
- d'activités de gestion, telle l'interruption des ventes et des paiements causée par l'infection des serveurs et des ordinateurs personnels des collaborateurs de l'entreprise ;
- d'activités commerciales, telle l'interruption causée par l'introduction d'un logiciel malveillant dans les systèmes d'information, qu'a subi la chaine de distribution américaine Target ;
- d'une interruption à l'initiative de l'entreprise, afin de conjurer une menace d'interruption des systèmes d'information ou d'en limiter la diffusion à l'intérieur de l'entreprise.

Les pertes d'exploitation pourront être constituées de pertes financières directes (perte de marge), décalées dans le temps (perte de clientèle ou d'opportunités) et/ou futures (suite à un cyber espionnage, perte de marge, dû à une nouvelle concurrence ou retard à mettre en place le business plan prévu).

Les frais de remise en état et de reprise d'activité pourront être significatifs. Ils peuvent consister en des :

- frais d'expertises « forensic » ;
- frais de réparation et de remise en état des équipements et installations informatiques ;
- frais de mise en conformité et de mise à niveau du système informatique ou des mesures de sécurité et organisationnelles requises par la législation, en particulier le RGPD ;
- dépenses d'investissement pour renforcer les mesures de défense et de résilience des systèmes d'information, suite à la survenance d'un incident de sécurité qui a révélé leurs insuffisances ;
- achats d'équipements,
- ainsi que des frais de mise à jour des matériels et des logiciels détruits, endommagés ou compromis, et mise à jour des outils de prévention (anti-virus, firewall, équipes RSSI et de surveillance [SOC ; détection, ...]).

Par ailleurs, l'entreprise pourra avoir à faire à des dépenses requises par l'autorité réglementaire agissant en matière de protection des données personnelles ou de sécurisation des données. Ces dépenses peuvent être liées à des frais de notification et frais juridiques, à la suite d'une procédure réglementaire engagée par l'autorité administrative ou encore des sanctions administratives prononcées par l'autorité administrative, suite à un incident de sécurité ou un « data breach ».

On peut y ajouter le coût d'une assurance des risques cyber.

b) Fraude

L'entreprise peut subir deux types de fraude, commise par un de ses employés, agissant seul ou avec la complicité d'un tiers, ou par un tiers agissant seul.

- **Les actifs immatériels de l'assuré**

L'acte de fraude peut viser les bases de données clients de l'assuré, les « business plan », les stratégies commerciales de l'entreprise, les données de recherche et développement et de manière plus générale, tout savoir-faire, pour autant que ces éléments aient été enregistrés sur des supports numériques.

- **Le détournement de sommes d'argent**

L'entreprise est vulnérable à tout détournement de sommes d'argent qui lui appartiennent ou qui se trouvent sous sa garde.

L'opération peut être commise au moyen de différents mécanismes. Une attaque directe par intrusion, installant dans les systèmes d'information de l'assuré, un logiciel malveillant qui pourra être activé pour donner ordre de virer une somme d'argent sur le compte de l'auteur de l'acte d'intrusion ou de tout complice.

La fraude peut s'opérer en mode indirect, par la récupération, notamment sur le « darknet », par l'auteur de l'intrusion, de données par « phishing », ou en mode direct, sur tous les supports informatiques sous le contrôle de l'entreprise, afin de perpétrer des détournements au détriment de celle-ci, mais aussi de ses fournisseurs et clients, susceptibles d'engager sa responsabilité pour défaut de sécurisation des données.

c) Atteinte à la réputation

Une attaque cyber, qu'elle ait été ou non couronnée ce succès, ou un incident de sécurité, médiatisé ou révélé à ceux qui auraient pu en être victimes (les titulaires de données), peuvent engendrer des pertes financières et requérir d'engager des frais considérables pour rétablir la réputation de l'entreprise.

En effet, la réputation est également un actif immatériel de l'entreprise, dont la valorisation est difficile à apprécier. Elle est composée, d'une part, d'éléments préexistants, tels qu'une base clients et des perspectives de vente incontestables, mais aussi, d'éléments virtuels, quand les produits et services ou certains d'entre eux, n'en sont qu'au stade de projets.

La réputation touche également à la confiance dans les produits et services de l'entreprise, tels que la facilité à accéder aux sites web ou à procéder à des paiements en ligne.

- **Pertes objectivement quantifiables**

Le montant des frais de réhabilitation de l'image de marque de l'entreprise peut varier fortement selon le mode de communication que l'entreprise retient. Il peut s'agir d'une communication de crise ciblée et limitée dans le temps, mais aussi d'une campagne médias, plus coûteuse, surtout si elle a pour ambition de faire savoir que l'entreprise revient sur le marché dans l'objectif de regagner un chiffre d'affaire perdu.

- **Pertes d'exploitation**

La détermination du lien de causalité entre l'incident et la perte d'exploitation est difficile à apprécier. Du point de vue de l'entreprise, on peut penser que seule la perte subie compte.

Toutefois, il faut prendre en considération le coût des contre-mesures pour réduire l'impact de ladite perte.

Par exemple, lorsqu'on soupçonne un concurrent de s'être approprié la technologie, les bases de données clients, ou d'avoir occupé un terrain en friche pour augmenter sa part de marché, il faudra engager des frais de recherche et développement élevés pour mettre sur le marché un produit ou un service qui se différencie de celui du concurrent.

- **Eléments subjectifs**

L'atteinte à la réputation peut avoir des impacts plus indirects. On peut citer deux exemples :

- pour les sociétés cotées, la baisse du cours de bourse, consécutive à une attaque cyber ou à une divulgation massive de données personnelles, qui mettrait en jeu le modèle économique de l'entreprise, à son image et qui se traduirait par la mise en cause des dirigeants sociaux ;

- l'imputation à l'entreprise d'un comportement illégal, et particulièrement du point de vue des discriminations (révélation de l'existence de fichiers ethniques ; refus d'accès aux sites internet, de vente ou de prestation à certaines catégories de population...).

2° Risques de dommages causés aux tiers – « Third party »

L'entreprise n'est pas uniquement la victime d'un incident de sécurité. Elle peut en relayer les effets sur ses clients ou des tiers, mais également être à l'origine d'un incident subi par un ou plusieurs tiers.

L'entreprise peut avoir à faire face à une procédure réglementaire, initiée par l'autorité de protection des données personnelles, telle que la Commission Nationale Informatique et Libertés (CNIL), au titre de la violation ou du non-respect du RGPD ou de toute législation sur la « Privacy » et les « data breach ».

L'entreprise peut également être responsable sur le plan civil, ou elle aura à répondre financièrement de ses actes ou omissions, que les victimes soient des entreprises, clientes ou non, ou des personnes privées.

a) Transmission de malware

L'entreprise est responsable de toute transmission d'un virus informatique ou d'un malware à un tiers. Cette transmission peut être passive, si elle relaye le logiciel malveillant reçu, sans avoir pu prévenir sa pénétration dans les systèmes d'information de l'assuré et empêcher sa transmission à partir de ceux-ci, ou active, le virus ayant été introduit volontairement ou involontairement, dans les systèmes d'information par un employé de l'entreprise.

b) Risque accidentel

L'entreprise est responsable des dommages causés à des tiers du fait de l'exercice de ses activités, de ses produits et services.

Les dommages peuvent prendre la forme :

- de dommages corporels, si l'attaque cyber s'est traduite, par exemple, par un accident de transport, un élément de sécurité (cf. équipement de signalisation...) ayant été compromis, ou par la contamination d'un produit, si le dosage de l'un de ses composants a été augmentésuite à la modification malveillante du protocole de fabrication (cf. attaque informatique contre équipements de traitement de l'eau en Floride) ;
- de dommages matériels, si l'incident de sécurité s'est traduit par un incendie chez des tiers, avec les conséquences financières de l'arrêt d'exploitation qui s'en est suivi ;
- de dommages immatériels, si l'incident de sécurité a donné lieu à une inexécution contractuelle, par exemple, un retard de livraison ou dans l'exécution des prestations ;
- des dommages de toute nature, consécutifs à un défaut du produit livré, causé par un virus informatique, qui fausse son fonctionnement (dans un objet connecté, par exemple), ou à une erreur de calcul, résultant de l'introduction d'un malware dans le logiciel de programmation et conduisant à l'inexécution d'une prestation professionnelle.

L'entreprise reste responsable de la bonne exécution des prestations, lorsque son sous-traitant est lui-même défaillant.

c) Responsabilités liées aux médias

En communiquant sur internet ou les réseaux sociaux, l'entreprise assume une responsabilité d'éditeur à l'égard des tiers, à tout le moins une responsabilité de contrôle des informations et messages diffusés sur ces supports.

L'atteinte aux droits des tiers peut relever des infractions suivantes :

- publication malveillante et dénigrement ;
- atteinte à l'image de l'entreprise ;
- atteinte à la marque, au design ;
- atteinte à la protection de la vie privée et à l'image d'une personne.

d) responsabilité liée aux données

- **Atteintes aux données confidentielles**

Se voyant confier des données et informations par un client ou un donneur d'ordre, l'entreprise est tenue de les restituer en l'état, de ne pas se les approprier et de les protéger de toute copie ou divulgation non autorisée. Elle assume toutes les conséquences financières directes et indirectes d'un tel manquement.

Lorsque les données ont une valeur particulière pour son détenteur ou pour les tiers, elles peuvent être protégées par des droits de propriété intellectuelle de tiers, qu'elles aient fait l'objet d'un dépôt ou qu'elles relèvent d'un secret des affaires.

- **Atteinte à la vie privée**

Lorsque l'entreprise doit répondre d'une violation à une législation sur la « Privacy » tel le RGPD dans l'Union européenne, elle peut être amenée, à engager des frais de notification aux victimes de la divulgation non autorisée de données à caractère personnel, ou à faire l'objet d'une lourde sanction administrative.

Les victimes du « data breach » peuvent également engager une action en responsabilité civile pour atteinte à la vie privée contre l'entreprise, individuelle ou collective, lorsque cette possibilité leur est ouverte (aux Etats-Unis, par exemple).

Une étude du consultant Kroll, « Global Fraud and Risk report 2019/2020 », donne certaines indications sur le rôle joué par les systèmes d'information dans les incidents survenus sur l'exercice d'étude. Si l'on prend en compte les facteurs les plus importants, ceux-ci ont été, le vol de données (49 %), la fuite d'informations internes (48 %) et le vol de données protégées par la propriété intellectuelle (43 %).

II – Les données à caractère personnel

Le souci de la protection des données à caractère personnel, selon le RGPD, désignées pour plus de simplicité comme données personnelles, s'est manifesté récemment, avec l'avènement de la société du numérique.

Elle a conduit à la généralisation d'une protection réglementaire spécifique tant aux États-Unis qu'en Europe, avec le Règlement Général relatif à la protection des données à caractère personnel (RGPD), et à l'ouverture progressive des ressources du droit de la responsabilité civile pour la réparation du préjudice subi par les victimes d'une atteinte à leur vie privée.

L'évaluation par un observateur, Ponemon Institute, des coûts de la divulgation non autorisée des données personnelles donnera la mesure des enjeux financiers d'un « data breach » pour l'entreprise.

A – La réglementation des États-Unis

Les États-Unis ne disposent d'aucune législation en matière de protection des données personnelles comparable à celle développée par l'Union européenne avec le RGPD. Leurs textes législatifs et réglementaires, ainsi que les protections et actions offertes aux détenteurs de données personnelles, sont d'inspiration très diverses, au plan fédéral comme au niveau des États fédérés.

1° La Constitution des États-Unis

La protection de la vie privée n'a été prise en compte que tardivement. Ainsi, le quatrième amendement du « Constitution's Bill of Rights » n'était censé protéger les personnes exclusivement contre l'intrusion du gouvernement dans leur vie privée et ne prévoyait pratiquement aucune mesure contre les agissements d'acteurs non gouvernementaux. Il stipule le droit des personnes à la sécurité de leurs biens, maisons, documents ainsi que leurs effets personnels contre les recours non raisonnables et les saisies.

Ce n'est qu'en 2018 que la Cour suprême des États-Unis a considéré que la protection de la vie privée des personnes contre l'intrusion du gouvernement s'étendait aux informations (en l'espèce des données de positionnement de téléphones d'un opérateur telecom), même lorsque celles-ci étaient partagées avec des tiers (Carpenter v. United States, 22 juin 2018, n°16-402).

Précédemment, la Cour suprême de 1977, « Whalen v. Roe », avait évoqué le droit à éviter certaines révélations, mettant en lumière, à propos de l'accès à des données de prescriptions pharmaceutiques, le droit à une « informational privacy », mais celui-ci n'a en fait jamais été reconnu (Whalen v. Roe, 22 février 1977, n° 75-839).

Tant les droits constitutionnels impliquant la « privacy » que le droit de la responsabilité civile en matière de vie privée (« common law privacy torts »), se concentrent sur la révélation publique de faits privés. Ils trouvent toutefois leurs limites dans la possibilité d'en faire application dans le monde des « data » d'aujourd'hui, à savoir leur collecte, la protection et l'usage des données.

2° Les législations fédérales en matière de données

Eu égard à ces insuffisances, le Congrès s'est attaché à élaborer des protections par la loi (« statutory protection ») des données personnelles des individus.

Il n'existe aucune protection générale, mais un ensemble de lois fédérales qui réglementent, directement ou indirectement, les pratiques des entreprises en matière de protection des données.

La plupart de ces lois imposent des obligations de protection des données sur des secteurs spécifiques d'activités, comme les institutions financières, les secteurs de la santé et des télécommunications, ou bien des types de données spécifiques, comme celles qui concernent les enfants.

Enfin, certaines législations bien que non limitées à la protection des données, peuvent restreindre la manière dont les sociétés peuvent traiter des données personnelles (par exemple, le « Federal Trade Commission Act »).

L'ASSURANCE DES LIGNES FINANCIÈRES

Les marchés classiques de l'assurance de « dommages aux biens » et de « responsabilité civile » peinent aujourd'hui à répondre à de nouvelles expositions de risques, pour certains transversaux.

De nouvelles polices, développées aux États-Unis sous la dénomination d'« assurance des lignes financières », protègent les actifs technologiques et financiers, les ressources et profits de l'entreprise et prennent en charge ses engagements en responsabilité civile à l'égard de nouvelles « victimes ».

Les polices d'assurance « lignes financières » s'inscrivent dans les nouvelles tendances réglementaires globales mises en œuvre par des autorités indépendantes, comme la SEC, l'AMF ou la CNIL.

Ces tendances sont soutenues par des tribunaux, par voie d'actions collectives, afin de faire appliquer des dispositifs juridiques innovants et exigeants, en matière boursière et de gouvernance d'entreprise, de protection des données personnelles, de lutte contre les discriminations et la corruption, en défense tant du bon fonctionnement des marchés financiers que des droits des actionnaires, des employés, des retraités et des personnes au respect de leur « privacy ».

Dans une approche comparative, cet ouvrage décrit les environnements juridiques, à la fois différents et convergents, français, de l'Union européenne et des États-Unis et les solutions que proposent les marchés d'assurance des « lignes financières » pour répondre à ces nouvelles problématiques.

Destiné aux professionnels du monde des affaires, de l'assurance et de la finance, ainsi qu'aux juristes, il permet de cerner les contours de la responsabilité civile des dirigeants et des mandataires sociaux, des responsabilités de l'entreprise en matière d'emploi et de protection sociale, de la fraude, des détournements d'actifs et des risques numériques.

Dominique Bercovici *est directeur « recherche et développement » du cabinet de courtage d'assurances Diot, filiale du Groupe Burrus, et président de Sanda Consulting. Il est titulaire d'une maîtrise de droit privé, d'un DEA en droit international privé et d'un DEA en droit communautaire et européen. Il a plus de 30 ans d'expérience dans le secteur de l'assurance des lignes financières des grandes entreprises, en compagnie et dans le courtage, en France et en Italie. Il enseigne les cyber risques dans le Master Spécialisé « Management global des Risques » de l'ENSAM.*

www.editionsargus.com

ISBN 978-2-35474-366-6

9 782354 743666