# ENJEUX

AUJOURD'HUI, LA GESTION DU CYBER-RISQUE EST DEVENUE INCONTOURNABLE. AVANT D'ÉLABORER UNE POLITIQUE ET DES PROCESSUS DE CYBERSÉCURITÉ, IL FAUT BIEN COMPRENDRE LE RISQUE ET SES IMPACTS.

« Les réseaux zombies (*botnets*) sont un atout extrêmement puissant pour les criminels, car ils peuvent être utilisés pour une grande variété de fins, telles que l'envoi de pourriels, le vol d'informations bancaires, la réalisation d'une attaque par déni de service distribué (*DDoS*) ou une variété d'autres activités malveillantes. »

— *Internet Security Threat Report 2014,* vol. 19, Symantec

# LE CYBER-RISQUE

## DE LA PRÉOCCUPATION À LA GESTION DU RISQUE

Le cyber-risque est devenu un réel enjeu : « Aujourd'hui, la question consiste à savoir quand et, surtout, comment le gérer », lance Amir Belkhelladi, associé leader de la pratique en cybersécurité, Est du Canada, chez Deloitte. L'approche des entreprises relativement à ce risque a évolué et « le cyber-risque figure maintenant dans le top 10 de leurs préoccupations ».

Le cyber-risque arrive également en tête des préoccupations actuelles du secteur canadien de l'assurance de dommages[1]. Pourtant, de nombreux sondages continuent à démontrer un manque de préparation et de protection à l'égard de ce risque[2]. À la fin de 2014, l'agence de notation A. M. Best révélait qu'au sein de l'industrie, près de 80 % des entreprises interrogées n'avaient aucune couverture contre le cyber-risque et que seulement 2 % des répondants s'étaient dotés d'un service spécialisé en cybersécurité[3].

« Depuis quatre à cinq ans, la probabilité que les cyberattaques soient efficaces, c'est-à-dire qu'elles se matérialisent, s'est fortement accrue », rappelle M. Belkhelladi. Le Canada est d'ailleurs une source de cybermenaces, comme le démontrent les classements de la firme de sécurité informatique Symantec: en 2013, le Canada était la quatrième source mondiale de menaces par hameçonnage, la huitième en matière de pourriels et la dixième pour l'envoi de virus par courriel[4]. En 2014, le Canada a également fait son entrée dans le groupe des 10 pays où les cyberactivités malveillantes se déroulent le plus au moyen de réseaux zombies[5].

### Ce qu'il faut savoir du cyber-risque

Les besoins d'éducation demeurent cependant importants. La rapidité avec laquelle le cyber-risque évolue en complique la gestion au sein de toutes les entreprises. Or, les plus petits cabinets et les représentants autonomes peuvent croire qu'il est trop difficile ou trop coûteux pour eux de suivre le rythme. Pour se protéger, il faut d'abord comprendre ce dont il s'agit. Voici quatre éléments dont il faut tenir compte :

**1. Toutes les entreprises peuvent être ciblées**

En 2014, les petites entreprises (de 1 à 250 employés) et les moyennes entreprises (de 251 à 2 500 employés) ont été la cible d'environ 60 % de toutes les attaques de harponnage (ou *spear-phishing*)[6], une variante sophistiquée de l'hameçonnage (*phishing*). Le harponnage consiste à envoyer un courriel qui semble provenir d'un client ou d'un employé de l'entreprise ciblée et qui contient suffisamment d'informations réelles (volées) pour que le message (piégé) semble légitime et crédible.

**2. Toutes les données peuvent être visées**

En 2014, les cinq types de données les plus exposées[7] étaient :

- les vrais noms des individus (et non leurs pseudonymes sur Internet);
- les numéros d'identification officiels (tels que les numéros d'assurance sociale);
- les adresses résidentielles;
- les informations financières;
- les dates de naissance.

Il est évident ici que toutes les entreprises œuvrant en assurance de dommages et en expertise en règlement de sinistres sont susceptibles d'être visées. « Il ne faut pas oublier que les cyberattaques se produisent aujourd'hui en quantité industrielle, explique Benoît Dupont, directeur scientifique du Réseau intégré sur la cybersécurité (SERENE-RISC) de l'Université de Montréal. On parle de plusieurs centaines de milliers d'attaques par jour. Les cybercriminels pénètrent d'abord les systèmes et ne se questionnent sur l'utilité des données volées qu'après les avoir obtenues. »

Par ailleurs, selon M. Dupont, non seulement les entreprises ne connaissent pas précisément la valeur de leurs données, mais « dans les faits, elles ignorent également combien de copies de ces données leurs employés ont pu faire pour faciliter leur travail, où ces duplicata se trouvent et ce qu'ils contiennent précisément ».

►►►

[1] Classé deuxième selon le communiqué « Le contexte réglementaire, le cyberrisque et les taux d'intérêt sont les principales sources de préoccupations du secteur canadien de l'assurance », 16 juillet 2015, PwC Canada, et troisième selon le *Deuxième sondage annuel sur les risques et les occasions dans le secteur de l'assurance au Canada*, KPMG.
[2] Voir article sur le sujet paru dans *La ChADPresse*, vol. 14, nº 3.
[3] *Cyber Security Presents Challenging Landscape for Insurers and Insureds*, A. M. Best, 2014.
[4] *Intelligence Report*, juin 2013, Symantec.
[5] *Internet Security Threat Report 2014*, vol. 19, Symantec, p. 45 et suivantes.
[6] *2015 Internet Security Threat Report*, vol. 20, p. 70, Symantec.
[7] *Id.*, p. 83.

L'AUTORITÉ DES MARCHÉS FINANCIERS PROPOSE UNE SÉRIE DE QUESTIONS QUI PERMETTRONT D'ALIMENTER LA RÉFLEXION ET DE METTRE EN PLACE DES MESURES DE PRÉVENTION ET DE SÉCURITÉ INFORMATIQUE. CONSULTEZ LE BULLETIN *INFO-CONFORMITÉ* (VOL. 4, Nº 4, OCTOBRE 2015) POUR EN SAVOIR PLUS.

**3. Antivirus et pare-feu ne suffisent pas**

Si les pare-feu et les antivirus sont importants, ils peuvent créer un faux sentiment de sécurité « face à des cyberpirates déterminés et motivés », mentionne M. Dupont. Pour être pleinement efficaces, les solutions informatiques doivent être mises à jour à la fois rapidement, soit dans les heures qui suivent la sortie d'une nouvelle mise à jour, et régulièrement.

S'il semble anodin de rappeler ces précautions, c'est qu'elles ne sont pas toujours suivies. Au printemps 2014, la faille Heartbleed a notamment forcé l'Agence du revenu du Canada à suspendre ses services en pleine période de déclarations fiscales. Une étude publiée en Australie a récemment révélé que 12 mois plus tard, près de 84 % des entreprises de ce pays n'avaient toujours pas corrigé la vulnérabilité de leurs systèmes à l'égard de ce bogue[8].

**4. Les mesures de sécurité de base sont gratuites**

Une perception tenace veut qu'une politique de cybersécurité coûte cher. « Pourtant, indique M. Dupont, l'une des mesures les plus importantes dans la gestion du cyber-risque, soit le maintien à jour des systèmes d'exploitation et des logiciels installés sur le réseau informatique, est en général gratuite ». Il mentionne d'ailleurs que les quatre stratégies qui contribuent à réduire de 85 % les tentatives d'intrusions ciblées peuvent être mises en place gratuitement[9]. Il s'agit de :

- la mise à jour du système d'exploitation;
- la mise à jour des logiciels et des applications;
- la restriction des privilèges d'administration du parc informatique à des professionnels spécialisés;
- le contrôle des logiciels et applications sur les postes informatiques en définissant une liste restreinte d'applications autorisées (*whitelisting*).

## Élaborer une politique de cybersécurité

Aujourd'hui, la gestion du cyber-risque est donc devenue incontournable. Avant d'élaborer une politique et des processus de cybersécurité, il faut d'abord « bien comprendre les probabilités que survienne le risque et ses impacts potentiels sur l'entreprise », explique M. Belkhelladi. Dans l'audit du risque, il faudra tenir compte des aspects réglementaires en vigueur, comme la protection des renseignements personnels.

Ensuite, il faut élaborer « des scénarios d'affaires avec des exemples concrets et adaptés à l'entreprise », soutient M. Belkhelladi. Ainsi, une attaque par déni de service rendra indisponible l'accès à un serveur Web ou à un site Internet ou encore la distribution de courriels. « Cela aura donc un impact sur les activités de l'entreprise, par exemple en empêchant les clients de faire une souscription en ligne. Cela s'accompagne aujourd'hui souvent de chantage pour recouvrer l'usage du réseau, ajoute M. Belkhelladi. Les vols de données liées à la propriété intellectuelle, comme une base de données actuarielle, ou de renseignements sur les clients (numéros de carte de crédit, coordonnées personnelles, etc.) posent, quant à eux, un risque réputationnel et commercial. »

La suite de l'exercice consiste à implanter des processus qui permettront de prévenir le risque, mais également de le détecter et de le contrôler, comme pour toute autre pratique de gestion de risque. Toutefois, l'élaboration d'une politique de cybersécurité ne correspond pas à une simple mise à jour de la politique de la gestion de risque existante où il suffit d'ajouter le terme cyber-risque ici et là. Il faut « reprendre la démarche depuis le début pour se doter d'une stratégie de gestion de crise adaptée au monde cyber, avec les ressources spécialisées adéquates », prévient M. Belkhelladi.

[8] *2015 Threat Report, Australian Cyber Security Centre*, p. 20.
[9] *Id.*, p. 18.

Les médias sociaux représentent aussi un canal propice aux cyberattaques (virus, pourriels, hameçonnage), en plus d'exposer les entreprises au risque réputationnel. Consultez la fiche-conseil de la ChAD pour élaborer une politique d'utilisation des médias sociaux à **chad.ca/outils**.

Compte tenu de l'ampleur de ce risque, « la répartition traditionnelle, avec un responsable pour chaque risque – financier, physique, juridique –, ne suffit plus, rappelle M. Dupont. Si vous êtes responsable des affaires juridiques, vous pourriez penser que le cyber-risque n'est pas de votre ressort. Pourtant, vous possédez probablement des données sur le fonctionnement de votre entreprise qui pourraient être cruciales. » Sans oublier que les membres du conseil d'administration (C. A.) pourraient se voir accusés d'avoir manqué à leur devoir fiduciaire ou de diligence en cas de cyberattaque.

L'affaire Wyndham aux États-Unis en est un exemple. Dans un premier recours, un actionnaire a tenté de poursuivre le C. A. de ce groupe hôtelier après le vol de renseignements personnels de plus de 600 000 clients lors de cyberattaques, accusant les administrateurs de ne pas avoir respecté leurs devoirs envers la société. Le C. A. a été blanchi dans la poursuite civile. Toutefois, la Commission fédérale du commerce (FTC) américaine vient d'être autorisée à intenter des poursuites réglementaires contre le groupe hôtelier à ce propos[10].

### Le facteur humain

Les politiques de cybersécurité devront donc tenir compte aussi de ceux qui devront l'appliquer. Selon le chercheur universitaire, « lorsque ces politiques sont trop contraignantes, les individus ont tendance à les contourner et à ne pas les respecter. Le changement fréquent de mot de passe peut ainsi les amener à choisir des mots de passe faibles, par lassitude ou parce que ces derniers sont plus faciles à mémoriser ». Selon lui, il serait alors préférable de changer les mots de passe moins souvent, si cela permet de s'assurer qu'ils restent forts.

« Même si on fournit aux représentants sur la route un ordinateur ultrasécurisé doté d'un accès par réseau privé virtuel, poursuit M. Dupont, ils sont susceptibles d'utiliser un réseau Wi-Fi gratuit dans un café », un type de réseau habituellement peu sécurisé. Pour qu'ils se sentent concernés par le rôle qu'ils ont à jouer dans la cybersécurité, il faut les outiller et les former régulièrement. Ils pourraient aussi recevoir une fiche qui résume la politique de cybersécurité en quelques points faciles à appliquer et qui cible les bonnes pratiques susceptibles de produire les effets les plus significatifs pour l'entreprise.

Il s'agit également de tenir compte de la culture au sein du cabinet. « Les personnes qui travaillent au développement des affaires sont reconnues pour leur prise de risque calculée, commente le chercheur. On ne peut pas leur demander du jour au lendemain de ne plus prendre aucun risque. » Les différents métiers devront donc être pris en compte lors de l'élaboration de la politique de cybersécurité. « Le cyber-risque est un changement majeur dans la gestion du risque dont les impacts touchent toutes les sphères organisationnelles, rappelle M. Dupont. Cela implique un changement de la culture de risque au sein des entreprises. » ■

## LE RÔLE DE L'INDUSTRIE

Aujourd'hui, le cyber-risque concerne non seulement les entreprises, mais aussi l'ensemble de l'économie, compte tenu des nombreuses interactions entre les acteurs économiques. Le Canada a d'ailleurs adopté une stratégie nationale en matière de cybersécurité[11]. Or, l'industrie de l'assurance de dommages a un rôle central à jouer, « comme elle l'a fait pour d'autres risques majeurs, commente M. Dupont. L'industrie est bien placée pour promouvoir les bonnes pratiques en vue de prévenir la cybercriminalité, comme elle l'a fait, par exemple, pour prévenir les incendies. »

En Europe, des collaborations ont été établies entre les firmes informatiques chargées de la sécurité des grands réseaux bancaires et l'industrie de l'assurance de dommages. L'objectif : partager les données liées au cyber-risque pour bâtir un modèle de prévision fondé sur des données fiables.

M. Belkhelladi explique aussi qu'au Royaume-Uni, « les organismes de réglementation simulent des cyberattaques sur les réseaux bancaires pour savoir comment réagir à un événement de cette ampleur ». L'Institut d'assurance du Canada a également souligné l'importance d'établir ces partenariats entre l'industrie et les gouvernements pour échanger des informations sur les menaces existantes et émergentes, les techniques de défense et les pratiques exemplaires[12].

[10] https://epic.org/amicus/ftc/wyndham.
[11] pensezcybersecurite.gc.ca.
[12] *Les cyberrisques : conséquences pour l'industrie de l'assurance au Canada*, Institut d'assurance du Canada, 2015, p. 46.