VOIR AU-DELÀ DU RISQUE

Canadian Institute of Actuaries / Institut canadien des actuaires

Bienvenue au nouveau numéro de *Voir au-delà du risque*, la publication trimestrielle électronique de l'Institut canadien des actuaires (ICA). Chaque numéro présente les plus récentes réflexions actuarielles de spécialistes. Patrick Vice, M.A.P., se penche ici sur les dangers en ligne auxquels sont confrontés les Canadiens et sur ce que peuvent faire les actuaires et d'autres professionnels pour vous aider à protéger vos finances des voleurs virtuels. Nous avons la certitude que vous trouverez cet article instructif et inspirant, et nous vous incitons à le partager avec vos amis et collègues.

Document 214116

LE RISQUE DANS LE CYBERESPACE – L'ASSURANCE CONTRE LE DANGER VIRTUEL

INTRODUCTION

Dans les années 1990, avant que l'Internet ne devienne un outil omniprésent dans l'entreprise, Sun Microsystems[1] utilisait le slogan « Le réseau, c'est l'ordinateur » pour faire la promotion de ses serveurs. L'une des réclames publicitaires mettait en vedette un très gros chien nommé Réseau, accompagné d'une explication qui ressemblait à ceci : « Comme tous les bons retrievers, Réseau ira chercher tout ce dont vous aurez besoin. »

Par **Patrick Vice**, M.P.A.

Aujourd'hui, au vu de la popularité de l'infonuagique, on pourrait dire que la vision de Sun s'est matérialisée, bien que quelques décennies plus tard. Toutefois, pour poursuivre l'analogie avec la race canine, il y a autant de pitbulls enragés que de gentils labradors : lorsque Spot rapporte l'information, il se peut qu'il mâchonne et avale une bonne partie de votre argent.

La menace que représentent les criminels et les fraudeurs en ligne ne fait qu'empirer. Les entreprises doivent se protéger contre divers risques, notamment la perte de données, la fraude, le piratage de sites Web, ainsi que le vol d'identités ou de la propriété intellectuelle. C'est pourquoi elles ont de plus en plus recours à des polices d'assurance contre les cyberrisques dans le cadre de leurs stratégies de sécurité et de gestion du risque d'entreprise.

Ce marché d'assurance connaît un certain essor et, en raison de l'évolution constante de ces risques et des possibilités d'exposition, les actuaires jouent un rôle indispensable auprès des assureurs, des courtiers et des gestionnaires du risque.

IMPORTANCE DU PROBLÈME

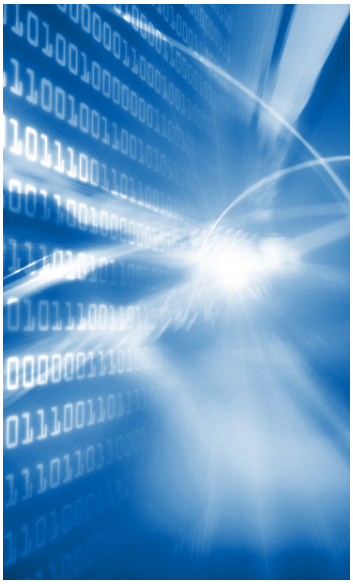
Les consommateurs, les entreprises et les administrations publiques se servent de la technologie pour accomplir leurs activités quotidiennes. Les deux dernières décennies ont vu une croissance exponentielle de l'Internet commercial afin d'accroître la disponibilité des ressources pour l'information et le commerce. En l'an 2000, 394 millions de personnes utilisaient l'Internet. Cette année, il est estimé que 2,9 milliards de personnes sont en ligne[2].

Le Canada continue de faire figure de chef de file à ce chapitre : les Canadiens passent en moyenne 45,6 heures par mois en ligne, contre 40,3 heures pour les Américains et 24,4 heures pour l'ensemble de la planète[3]. En conséquence, les particuliers et les

SUITE À LA PAGE 2

1. Fait aujourd'hui partie intégrante d'Oracle.
2. Statista.
3. Autorité canadienne pour les enregistrements Internet, Dossier documentaire 2013.

Les cinq plus grandes cybermenaces pour les assureurs[4]



- **Attaques de plus en plus sophistiquées.** La fréquence et la sophistication des cyberattaques sont en hausse.
- **Faible défense du périmètre.** La plus grande disponibilité des systèmes et des données au moyen des appareils mobiles, des portails en libre service et des services partagés augmente le nombre de « surfaces d'attaque » que les assureurs doivent protéger.
- **Mauvaise utilisation des ressources en matière de sécurité.** La plupart des entreprises se servent des mêmes outils pour protéger les réseaux, les systèmes et les données, mais ces outils ne sont pas une solution lorsqu'ils sont mal utilisés.
- **Négligence des utilisateurs finaux.** Même les utilisateurs finaux bien intentionnés sont négligents.
- **Absence d'harmonisation entre les impératifs informatiques et opérationnels.** Il est essentiel d'établir une bonne communication entre les partenaires de l'entreprise sur le plan de la gestion et de l'atténuation des risques.

entreprises s'exposent à des cybermenaces issues de diverses sources. Selon la **Stratégie de cybersécurité du Canada** :

- 59 % des déclarations d'impôt sur le revenu ont été transmises par voie électronique en 2008 (75 % en 2013[5]);
- 67 % des Canadiens ont effectué des opérations bancaires en ligne en 2009 (77 % en 2014[6]);
- En 2007, les ventes en ligne au Canada étaient évaluées à 62,7 milliards de dollars (136 milliards de dollars en 2013[7]).

Dans son message accompagnant la Stratégie, l'honorable Vic Toews, alors ministre de la Sécurité publique, avait écrit :

> Les Canadiens (individus, industries et gouvernements) sont conscients des nombreux avantages qu'offre le cyberespace pour notre économie et qualité de vie. Notre grande dépendance aux cybertechnologies nous rend toutefois plus vulnérables aux attaques lancées contre nos infrastructures numériques dans le but de déstabiliser notre sécurité nationale, notre prospérité économique et nos modes de vie.

Selon le **Rapport Norton 2013**, on estime à trois milliards de dollars américains le coût total de la cybercriminalité au Canada. En janvier 2012, Bob Paulson, commissaire de la Gendarmerie royale du Canada (GRC), avait écrit à Steven Blaney, ministre de la Sécurité publique et de la Protection civile, afin que le gouvernement donne aux Canadiens de plus amples informations sur les moyens de se protéger sur Internet, et qu'il étende les pouvoirs des organismes d'application de la loi en la matière. M. Paulson avait écrit : « Cette menace grandissante nuit grandement à la prospérité nationale et affecte autant les Canadiens. »

Le cyberpiratage et la cybersurveillance ont connu un essor proportionnel à l'évolution du commerce sur Internet. En 1994, Vladimir Levin et un groupe de pirates russes ont viré illégalement 10 millions de dollars américains de Citibank vers des comptes à l'étranger. Levin a été arrêté, jugé puis condamné par un tribunal américain. On a finalement pu récupérer la plus grande partie des fonds[8].

Maintenant, avançons rapidement jusqu'en 2014. Mt. Gox, une plateforme d'« échange de bitcoins » (système de monnaie virtuelle), a été l'objet d'un piratage, ce qui a entraîné des pertes de près de 500 millions de dollars américains. En juin, le

SUITE À LA PAGE 3

4. **Insurance Networking** (accès par abonnement seulement).
5. **Agence du revenu du Canada**.
6. **Association des banquiers canadiens**.
7. **CBC**.
8. **Wikipédia** et le **FBI**.

fondateur de Mt. Gox a déclaré que seuls 23 % des bitcoins ont été récupérés, et qu'il ne pensait pas pouvoir en retrouver d'autres. Mt. Gox fait actuellement l'objet d'une procédure de liquidation judiciaire[9].

Le cybercrime ne touche pas seulement les opérations commerciales et les particuliers. Plus tôt cette année, on a **appris** que le Conseil national de recherches avait été piraté par ce que l'on a décrit comme étant « un acteur chinois très sophistiqué parrainé par l'État ». En raison de cette intrusion, le système informatique du Conseil a dû être isolé afin de protéger les autres ministères. Au cours des années précédentes, des organismes canadiens importants tels que Recherche et développement pour la défense Canada ont eux aussi été l'objet d'**attaques** dans le cyberespace.

Dans son **étude de 2014 sur le coût des intrusions**, le respecté institut Ponemon a fait savoir que, aux États-Unis, la violation de données coûtait en moyenne, par entreprise, 3,5 millions de dollars américains, ce qui représente une hausse de 15 % par rapport à l'année précédente, coûts directs et indirects compris. Ce qui coûte le plus cher, c'est la réparation des dommages causés à la réputation de l'entreprise ainsi que par la perte de clients fidèles. Plus tôt cette année, on estime que le vol très médiatisé des données des cartes de crédit chez Target aurait coûté à l'entreprise au-dessus d'un milliard de dollars américains[10]. Les estimés actuels se chiffrent à 148 millions de dollars américains[11].

Au fur et à mesure que la technologie Internet étendra son rayonnement, les risques s'en trouveront accrus. **Business Insider** décrit la prochaine évolution de la connectivité du point de vue fonctionnel : [traduction] « L'Internet des objets fera en sorte qu'un grand nombre des appareils et objets qui nous sont familiers – depuis les serrures de porte jusqu'aux postes de péage en passant par les réfrigérateurs – seront du jour au lendemain branchés à Internet, accessibles par téléphone intelligent et adaptatifs », permettant ainsi aux usagers légitimes d'exercer un plus grand contrôle. Cela en fera aussi une cible plus attrayante pour les cybercriminels.

RÉACTIONS DES ASSUREURS ET DES AUTRES ACTEURS

L'apparition de l'Internet commercial dans le milieu des années 1990 a suscité un intérêt grandissant dans la vente de produits et services en ligne, ce qui n'a pas tardé à soulever des inquiétudes au sujet des risques, et a offert la possibilité de vendre de l'assurance contre ces risques. Dans les premiers temps, le marché a été difficile. Toutefois, avec l'expansion du commerce électronique et l'émergence des risques s'y rapportant, en plus des pressions exercées par de tierces parties, dont les gouvernements, un marché s'est développé pour des produits d'assurance sophistiqués.

En 1999, le magazine *Canadian Underwriter* avait **publié un article** au sujet d'un débat que la Society of Chartered Property Casualty Underwriters (société américaine) avait organisé et qui portait sur l'assurance et le commerce électronique. En référence à l'essor du commerce électronique, Jeff Behm, d'Atlantic Mutual, avait fait remarquer que cela créerait de la demande pour de nouveaux produits d'assurance. De l'avis de celui-ci, les principales inquiétudes des assurés potentiels étaient la perturbation des activités causée par les intrusions, ainsi que la perte de données.

Or, au cours de la décennie suivante, les ventes ont été inférieures aux attentes. Selon Sarb Sembhi, rédacteur attitré du *ComputerWorld*, cette réaction initiale s'explique de **deux façons** : « Le manque de données utiles à la souscription et le manque de connaissances qui aurait permis aux consommateurs de bien comprendre les avantages que représente le transfert des risques. »

Les événements très médiatisés, tels que le vol des données des cartes de crédit chez Target et, plus récemment, celui des données d'Home Depot, ou encore le **vol en ligne** de 900 numéros d'assurance sociale dans le système de l'Agence du revenu du Canada, permettent de sensibiliser la population aux cyberrisques.

M. Sembhi a fait remarquer que l'assurance cyberresponsabilité actuellement offerte sur le

SUITE À LA PAGE 4

9. **Reuters**.
10. **TwinCities.com**.
11. **Forbes**.

marché répondait mieux aux besoins des entreprises clientes, du fait des caractéristiques suivantes :

- Protection contre la violation de données et aide en matière de gestion des crises;
- Garantie de responsabilité relative aux médias et aux multimédias;
- Garantie de responsabilité en matière d'extorsion;
- Garantie de responsabilité relative à la sécurité des réseaux.

Les gouvernements incitent aussi les entreprises commerciales à renforcer la sécurité de leurs données. Aux États-Unis, 46 États ont adopté une **loi** exigeant la déclaration des cas de violation de données, et le gouvernement Obama envisage l'adoption d'une loi fédérale. En mars, l'Union européenne a voté en faveur d'un règlement pour protéger les données. Les amendes proposées vont jusqu'à 100 millions d'euros ou 5 % du chiffre d'affaires mondial, en fonction du montant le plus élevé.

Pour les cadres supérieurs des sociétés d'assurance, les cyberrisques représentent une nouvelle occasion d'affaires. Selon un **livre blanc** produit par Crawford and Company, les primes d'assurance contre les cyberrisques ont totalisé aux États-Unis 1,3 milliard de dollars en 2013. Broker Marsh a **estimé** que ce chiffre pourrait atteindre, en 2014, deux milliards de dollars.

Les assureurs introduisent de nouveaux produits sur le marché, mais en faisant preuve de prudence. Selon le document de Crawford and Company : [traduction]

> « Les assureurs ne disposent pas à l'heure actuelle des données et des statistiques sur les réclamations lui permettant de brosser un portrait exact de l'exposition, et c'est pourquoi ils ne sont pas intéressés à offrir une formule étendue qui indemniserait entièrement les assurés et les tiers contre les cyberrisques… Rares sont les assureurs en mesure d'offrir des indemnités supérieures à 50 millions de dollars, et la plupart d'entre eux offrent des garanties maximales d'au plus 10 millions de dollars. »

Quoi qu'il en soit, les pressions du marché devraient entraîner avec le temps une extension de la couverture et une hausse des garanties maximales.

QUE FONT LES ACTUAIRES POUR PROTÉGER LES PARTICULIERS ET LES ENTREPRISES?

Compte tenu de la complexité des profils de risque, de la nouvelle nature des menaces, de l'environnement dynamique des technologies fondamentales et de l'importance des expositions, les actuaires ont un rôle à jouer aussi difficile qu'essentiel. Heureusement, il existe un corpus de connaissances qu'ils peuvent consulter. Les modèles actuariels servant à calculer le risque de cyberattaques et le montant des primes d'assurance contre ce risque ne cessent d'évoluer, et cette année,

SUITE À LA PAGE 5

Depuis quelques années, on mentionne de plus en plus le travail et les responsabilités de l'actuaire dans les lois et la réglementation gouvernementales. Dans la plupart de ces documents, le terme « actuaire » y est défini comme un Fellow de l'Institut canadien des actuaires.

des actuaires, dont certains sont membres de l'ICA, ont créé un **groupe d'étude** chargé d'effectuer des recherches sur les activités et d'offrir des possibilités de formation en matière d'analyse des cyberrisques. D'autres actuaires ont donné des ateliers et des exposés sur le sujet.

Certains **experts** croient que, au fur et à mesure que les nouveaux cas de violation de données seront portés à la connaissance du grand public, la disponibilité des nouvelles statistiques permettra d'améliorer la valeur des modèles des actuaires, rendant ainsi leur rôle de plus en plus important.

CONCLUSION

La croissance continue de l'adoption de la technologie Internet s'accompagnera d'une hausse des risques financiers pour les particuliers, les entreprises et les administrations publiques, et bien entendu, d'une hausse des risques pour la sécurité de la population. Bien qu'il soit très difficile de comprendre et de gérer ces risques, soyez assurés que la communauté actuarielle et les sociétés d'assurance de premier plan étudieront ces questions en parallèle, afin d'avoir une compréhension commune lorsque le marché et les profils de risque seront mieux définis.

Patrick Vice possède plus de 25 ans d'expérience dans le commerce technologique et électronique des communautés de la gestion du risque et de l'assurance. Associé fondateur d'Insurance-Canada.ca, source principale de nouvelles en matière de technologie et d'assurance, il a occupé des postes de haute direction au sein de sociétés d'assurance, de distributeurs, de cabinets d'experts-conseils et de fournisseurs de solutions technologiques. Il siège à des conseils d'administration et des comités de plusieurs associations de l'industrie et il rédige également des articles pour des publications spécialisées de premier rang.