La cyberatteinte :

un risque très présent dans le secteur de la santé

Imaginez pendant un moment que vous arrivez au travail et que vous ouvrez votre ordinateur seulement pour constater qu'il a été infecté par un virus. Le virus a compromis les renseignements personnels sur la santé et les données de facturation de centaines de clients. Et, de plus, les renseignements personnels de vos employés ont aussi été compromis, y compris leur numéro d'assurance sociale et leurs informations bancaires.

Ou imaginez que quelqu'un s'est introduit par effraction dans votre voiture et a volé votre ordinateur portable qui contenait des renseignements sur vos clients actuels et antérieurs, y compris leur nom, leur adresse, leur numéro de téléphone et leurs renseignements personnels sur la santé.

Ou encore cette situation : À la demande de votre client, vous acceptez d'envoyer son dossier clinique par télécopieur à un tiers. Malheureusement, vous entrez le mauvais numéro de télécopieur et les renseignements personnels sur la santé sont télécopiés par erreur à une autre personne.

Que devez-vous faire? Quels sont vos responsabilités professionnelles et comment répondez-vous à ces atteintes à la vie privée?

Selon Beazley SPRL (Beazley)[1], un chef de file de l'assurance pour les interventions en cas d'atteintes aux données, la divulgation non intentionnelle de dossiers – comme un courriel mal adressé – était la principale cause des atteintes aux données dans le secteur de la santé en 2016 et en 2017. Les atteintes non intentionnelles représentent 41 % du nombre total des atteintes signalées à Beazley par des organismes du secteur de la santé. Or, ce niveau élevé n'a pas été résolu et il constitue plus du double de la deuxième cause des pertes, soit le piratage ou les logiciels malveillants (19 %). Le piratage et les logiciels malveillants (y compris l'extorsion informatique) demeuraient la cause la plus importante d'atteinte aux données affectant tous les secteurs avec 34 % du total des atteintes signalées à Beazley au cours des premiers mois de 2017.

Rançongiciels et cyberextorsion à la hausse dans le secteur de la santé

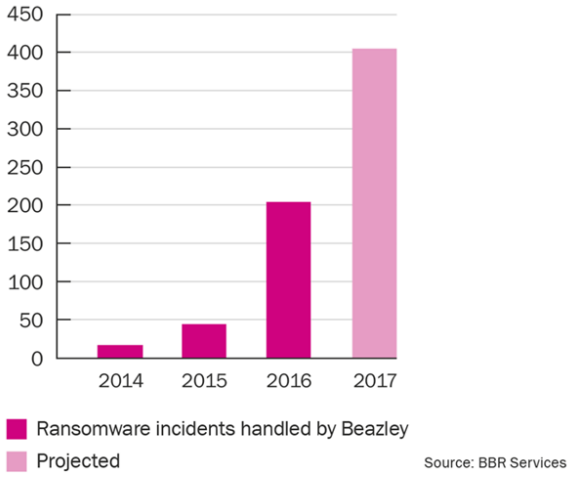
Les pirates ont de plus en plus recours aux rançongiciels pour bloquer l'accès aux données d'une organisation jusqu'à ce qu'une rançon soit versée en Bitcoin, une monnaie pratiquement impossible à retracer. L'établissement Hollywood Presbyterian Hospital à Los Angeles a signalé qu'il avait subi une attaque de rançongiciel en février 2016 et il a finalement versé 17 000 $ en Bitcoin aux pirates.

L'année précédente, le FBI avait émis une alerte signalant que les attaques de rançongiciels étaient en hausse.

Cette tendance est appuyée par les données de Beazley. Parmi les clients de Beazley, les atteintes par rançongiciels ont plus que quadruplé pour un total de plus de 200 atteintes en 2016 et la tendance s'est accélérée en 2017.

« Clairement, les nouveaux logiciels malveillants, y compris certains rançongiciels, ont un impact important », a dit Paul Nikhinson, gestionnaire des services d'intervention en cas d'atteintes à la vie privée chez BBR Services. « Le secteur de la santé représente une cible importante pour les pirates en raison de la richesse des dossiers médicaux pour le vol d'identité et d'autres crimes », a ajouté Nikhinson. « En fait, la valeur d'un dossier médical est plus de 16 fois supérieure à celle d'un dossier de carte de crédit. » [2]

Attaques de rançongiciels gérées par Beazley



Quelles sont vos responsabilités?

À titre de praticien de la santé, vous êtes responsable de la protection de la confidentialité et de l'intégrité des renseignements personnels, médicaux et financiers de votre client pendant qu'il est confié à vos soins et à votre gestion. Ces mesures de protection doivent être physiques (p. ex., classeurs verrouillés), organisationnelles (p. ex., politiques, autorisations de sécurité) et technologiques (p. ex., cryptage, protection par mot de passe). Si les renseignements des clients ont été perdus, volés ou consultés d'une autre façon par des personnes non autorisées, vous pourriez aussi être responsable d'en informer votre organisme de surveillance de la vie privée (c'est-à-dire le Commissaire provincial à l'information et à la protection de la vie privée) et/ou votre organisme de réglementation. [3]

Vous devriez aussi vous familiariser avec les politiques et les procédures en milieu de travail qui se rapportent à l'atteinte à la vie privée, notamment sur des sujets comme la formation sur la vie privée, la gestion de l'accès, la gestion des atteintes à la vie privée et les mesures disciplinaires.

Quels sont les coûts potentiels d'une cyberatteinte?

Si vous avez fait l'objet d'une cyberatteinte, votre client pourrait vous tenir légalement responsable des dommages financiers et des torts émotionnels dont il a été victime lorsque des renseignements personnels sur la santé et/ou des données de facturation ont été divulgués de manière inappropriée. En plus de l'indemnisation de votre client pour ces dommages, vous engagerez probablement d'autres coûts qui incluraient notamment ceux reliés à l'embauche d'un expert en sécurité informatique afin de déterminer la cause de l'atteinte aux données électroniques, à la notification des personnes dont les renseignements ont été compromis, à l'atténuation des atteintes à la réputation ainsi qu'à la défense ou aux sanctions en lien avec les infractions à la Loi sur la vie privée.

On estime que le coût moyen d'une cyberatteinte dans le secteur de la santé s'élève à 359 $ US par dossier, soit le coût le plus élevé pour toutes les catégories d'industrie.[4] Lorsque l'on multiplie ce chiffre par des dizaines, voire des centaines de dossiers de clients qui pourraient être consultés notamment sur une clé USB ou un ordinateur ou encore dans la base de données du bureau, les coûts peuvent grimper rapidement et être dévastateurs pour le psychologue moyen.

Face à ce nouveau risque, l'assurance cyber-responsabilité et atteinte à la vie privée peuvent être d'un secours considérable.

En tant que participant au programme d'assurance de la SCP ou du CSPP, vous bénéficiez d'une certaine protection dans le cadre de votre police d'assurance responsabilité professionnelle, dont une couverture de 50 000 $ pour chaque incident de cyber-responsabilité et d'atteinte à la vie privée. Cela signifie que vous avez déjà une certaine protection pour les réclamations causées par la perte ou la divulgation de renseignements des clients.

Cependant, une atteinte aux données peut être dispendieuse et peut éventuellement coûter des centaines de milliers de dollars. Pour une meilleure protection, les membres de la SCP et du CSPP ont aussi accès à une assurance cyber-responsabilité et atteinte à la vie privée additionnelle conçue spécifiquement pour les professionnels de la santé afin de vous aider à gérer le risque inhérent à la conservation de grandes quantités de données personnelles identifiant les clients, les employés et d'autres personnes et à atténuer les torts causés à la réputation découlant d'une atteinte à la sécurité informatique. Cette couverture facultative est offerte en partenariat avec BMS Canada Services de risque Ltée (Groupe BMS) et est émise par Beazley.

Quelle est la protection offerte par l'assurance cyber-responsabilité et atteinte à la vie privée?

La police d'assurance facultative de cyber-responsabilité et d'atteinte à la vie privée comprend la couverture suivante :

- Limite totale de 1 million $
- Paiement des dommages-intérêts à un tiers, y compris les dépenses juridiques;
- Coûts associés à l'enquête sur la cause de l'atteinte;
- Coûts associés à la notification des personnes touchées par l'atteinte;
- Coûts pour récupérer ou remplacer les données compromises;
- Paiement de rançons pour récupérer les données cryptées;
- Coût de l'interruption des activités en raison de la cyberatteinte;
- Équipe d'intervention spécialisée incluant des experts en informatique, des services juridiques ainsi que des services de notification et d'atténuation de l'atteinte;
- Coûts associés à la gestion de la crise et aux relations publiques;
- Couverture pour le coût de la défense auprès de l'organisme de réglementation et des sanctions qui pourraient découler des infractions à la Loi sur la vie privée.

Stratégies de gestion des risques

Les attaques réussissent souvent en exploitant des systèmes mal configurés ou des erreurs humaines, comme en incitant les employés à répondre à des courriels hameçons. En plus de se procurer la couverture d'assurance appropriée, voici cinq mesures que les entreprises du secteur de la santé peuvent prendre pour appuyer la protection des données :

1. Formez les employés à être conscients des renseignements qu'ils doivent protéger, informez-les à propos des meilleures pratiques, des principes et des normes en matière de protection de la vie privée et de la confidentialité – et sur la façon dont ils peuvent éviter les attaques par courriel hameçon et d'autres formes d'ingénierie sociale.[5]

2. Mettez au point un plan robuste pour intervenir en cas d'incident. Les atteintes aux données ne peuvent être gérées de façon impromptue. La planification préalable peut permettre d'éviter de graves torts à la réputation et aux finances. Un plan d'intervention bien pensé et testé devrait guider les gestionnaires pendant le cycle de vie d'une atteinte – à partir du premier soupçon de problème jusqu'à l'analyse judiciaire complète, en passant par les conseils juridiques, la communication avec les clients et l'assistance pour les relations publiques.[6]

3. Établissez une catégorisation des risques potentiels pour les données en fonction du niveau de la menace. Une réaction exagérée face à une atteinte peut être tout aussi dommageable qu'une réaction insuffisante. [7]

4. Examinez attentivement les contrats des fournisseurs afin de veiller à ce que les données de vos clients soient protégées lorsqu'elles se trouvent entre les mains des fournisseurs.

5. Chiffrez vos données et permettez la suppression des données (à distance lorsque cela est possible), particulièrement sur les appareils mobiles, les portables et les clés USB, qui seront plus susceptibles d'être perdus ou volés.[8]

Pour en savoir davantage à propos des risques informatiques ou pour souscrire une assurance de cyber-responsabilité et d'atteinte à la vie privée, veuillez contactez le Groupe BMS au 1-855-318-6038 ou à psy.insurance@bmsgroup.com.

Bibliographie :

1. Rapport Beazley. Juillet 2017. https://www.beazley.com/news/2017/beazley_breach_insights_october_2017.html
2. Rapport Beazley. Mars 2016. https://www.beazley.com/news/2016/beazley_breach_insights_2016_shows_sharp_increase_in_hacking_and_malware.html
3. Pour en savoir davantage à propos des lois sur la vie privée fédérales et provinciales et les normes de pratiques à cet égard, veuillez communiquer avec votre ordre professionnel. Le Commissariat à la protection de la vie privée du Canada fournit aussi des ressources pour les personnes et les organisations, dont une liste de contrôle en cas d'atteinte à la vie privée, un livret et des renseignements sur les mesures à prendre pour intervenir lors d'une atteinte à vie privée : https://www.priv.gc.ca.
4. Étude 2014 sur le coût des atteintes informatiques du Ponemon Institute. http://ponemon.org
5. Ressource : https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf
6. Ressource : https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/how-good-is-your-cyberincident-response-plan
7. Ressource : https://www.securestate.com/blog/2012/04/03/data-classification-why-is-it-important-for-information-security
8. Ressource : https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/PublicSectorBenelux/deciphering-the-code-a-simple-guide-to-encryption-wpna-(2).pdf?la=en