CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Cybersécurité et protection des données

TENDANCE TECHNOLOGIQUE

De nos jours, plus de 6 millions de données sont volées ou perdues quotidiennement[1]. Pour atténuer les dommages causés, 6 T$ seront dépensés à l'échelle mondiale d'ici 2021[2]. Par ailleurs, des modifications apportées à la législation canadienne sur la protection des renseignements personnels font que les entreprises doivent désormais investir dans la protection des données[3]. *Et vous, avez-vous pensé à votre budget de sécurité?*

Description

Plus des trois quarts des entreprises canadiennes de toute taille appréhendent une augmentation des cyberattaques, mais moins de la moitié prévoient accroître leur budget de sécurité afin de respecter leurs propres exigences en matière de conformité et de protection des données. Et peu sont prêtes à affronter une hausse de ce type d'attaques. Pourtant, elles risquent gros, car elles s'exposent à des amendes de 100 000 $ en cas d'irrégularités dans le signalement d'une atteinte à la vie privée (LPRPDE[4]) et de 10 M$ pour des messages commerciaux non sollicités contenant un logiciel malveillant (LCAP[5]). Elles pourraient aussi encourir des pénalités de plus de 60 M$ (peu importe le continent

1 Depuis 2013, on compte l'équivalent de 6 061 622 vols de données par jour (soit 252 568 par heure, 4 209 par minute ou 70 par seconde). Source : https://breachlevelindex.com (page consultée le 26 août 2019).

2 À l'échelle mondiale, les dépenses en cybersécurité devraient atteindre près de 6 T$ d'ici 2021. Les organisations doivent repenser leur approche en matière de cybersécurité et revoir leurs priorités budgétaires afin de tenir compte de cette nouvelle réalité de notre société moderne. www.forbes.com/sites/forbestechcouncil/2018/11/09/how-not-to-waste-a-trillion-dollars-on-cybersecurity/

3 www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd_pb_201810/

4 La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) est la loi fédérale canadienne de protection des renseignements personnels. Elle régit la façon dont les entreprises gèrent les renseignements personnels dans le cadre de leurs activités commerciales.

5 La *Loi canadienne anti-pourriel* (LCAP) est une loi fédérale qui protège les consommateurs et les entreprises contre les pourriels et les menaces électroniques.

où elles se trouvent) si, par leur mauvaise gestion des renseignements personnels de résidents européens, elles enfreignent le Règlement général sur la protection des données (RGPD[6]) de l'Union européenne. De plus, les cybermenaces (logiciels malveillants, hameçonnage, rançongiciels, etc.) continuent d'apporter leur lot de nouveaux risques.

Peu importe leur secteur d'activité, rares sont les gestionnaires et les administrateurs qui savent que la Loi sur la protection des renseignements personnels numériques a élargi les responsabilités prévues dans la LPRPDE afin d'y inclure l'obligation de signaler toute atteinte à la sécurité des données. Il y a donc des risques de litige, en plus des amendes mentionnées précédemment.

Certaines entreprises canadiennes profitent pleinement de cette occasion pour sécuriser leurs pratiques, protéger les données de leurs clients et prendre de l'avance sur la concurrence en démontrant qu'elles respectent les normes de sécurité. En plus d'astreindre les organisations à aviser l'intéressé de toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels le concernant, s'il est raisonnable de croire que l'atteinte présente un risque réel de préjudice grave à son endroit, la Loi sur la protection des renseignements personnels numériques exige maintenant que ces mêmes organisations tiennent et conservent un registre de toutes les atteintes aux mesures de sécurité qui ont trait à des renseignements personnels.

Cependant, pour signaler une telle atteinte, il faut d'abord la détecter. Cela signifie que, pour gérer les atteintes à la sécurité des données et s'acquitter de leurs obligations, les entreprises doivent investir dans la sécurité, c'est-à-dire dans les contrôles internes et la surveillance.

Importance

Les cybermenaces et les atteintes à la sécurité des données peuvent mettre à mal une réputation et causer de grandes pertes financières. La version révisée de la LPRPDE prévoit des amendes pouvant atteindre 100 000 $ lorsqu'une entreprise canadienne omet d'aviser convenablement les consommateurs et le commissaire à la protection de la vie privée d'une atteinte aux mesures de sécurité. Depuis le 1er novembre 2018, les entreprises canadiennes qui conservent, traitent, contrôlent ou gèrent des renseignements personnels doivent en effet s'assurer d'aviser les personnes touchées par ces atteintes.

Il faut agir dès maintenant. Selon une étude récente[7], les principaux facteurs ayant une incidence sur les dépenses des organisations en matière de sécurité sont les suivants :

6 Le Règlement général sur la protection des données (RGPD) de l'Union européenne, qui est entré en vigueur le 25 mai 2018, traite de la protection des données et des renseignements personnels.

7 Étude d'IDG sur les priorités en matière de sécurité pour 2018. https://resources.idg.com/download/executive-summary/security-priorities-2018

- Besoin d'établir ou d'appliquer des pratiques exemplaires (74 % des répondants);
- Respect des obligations de conformité (69 % des répondants);
- Réponse à un incident de sécurité qui s'est produit au sein de l'organisation (36 % des répondants);
- Mandat provenant du conseil d'administration (33 % des répondants);
- Réponse à un incident de sécurité qui s'est produit au sein d'une autre organisation (29 % des répondants).

Les organisations qui misent sur la préparation seront mieux outillées, ce qui leur procurera de nombreux avantages, notamment sur le plan concurrentiel.

Considérations pour les entreprises

Préparation

Fait intéressant à noter, 43 % des cyberattaques ciblent des entreprises et des professionnels comptables. Après avoir fait un bon travail d'introspection et pris les mesures nécessaires pour se conformer aux exigences, il est plus facile de communiquer et d'échanger avec d'autres organisations qui se trouvent dans des situations similaires. Par ailleurs, communiquer avec le Commissariat à la protection de la vie privée pour présenter son entreprise est un excellent moyen d'établir rapidement une relation avec les autorités, d'accéder à des ressources officielles et d'éviter de travailler en vase clos. Les entreprises sont certes responsables de leurs activités et de leurs actions, mais elles peuvent compter sur un partenaire clé, soit le commissaire à la protection de la vie privée. Celui-ci peut leur offrir une aide et des ressources précieuses bien avant qu'elles ne soient nécessaires.

Le plus grand avantage d'une bonne préparation réside dans la réduction du nombre d'erreurs humaines. En effet, 95 % des atteintes à la cybersécurité découlent d'une erreur humaine[8], ce qui laisse croire que de nombreuses cyberattaques ne sont pas purement d'ordre technologique : le facteur humain entre aussi en jeu. En fait, 64 % des entreprises ont déjà subi des attaques sur Internet et 62 % ont été la cible de techniques d'hameçonnage et de piratage psychologique. D'où l'importance des activités de sensibilisation et de formation continue des employés, telles que les campagnes de sensibilisation aux cybermenaces et les semaines de la prévention de la fraude.

Détection et surveillance

Il existe aujourd'hui des sauvegardes éprouvées en matière de cybersécurité auxquelles les entreprises canadiennes et les professionnels exerçant à titre individuel peuvent avoir recours pour assurer leur propre protection et celle de leurs clients; aux États-Unis, les

8 Les atteintes à la cybersécurité sont causées dans 95 % des cas par une erreur humaine. Pour s'infiltrer dans votre entreprise, les cybercriminels et les pirates informatiques exploitent les failles de sécurité (qui ne sont presque jamais attribuables au service des TI). www.cybintsolutions.com/cyber-security-facts-stats/

atteintes à la sécurité des données sont signalées depuis belle lurette (plus précisément, depuis l'entrée en vigueur, le 1er juillet 2003, de la loi californienne SB1386). Au Canada, cependant, les entreprises commencent tout juste à se familiariser avec leurs obligations légales en ce qui a trait à la détection des atteintes aux mesures de sécurité et à leur signalement au commissaire à la protection de la vie privée et aux personnes touchées. Autrement dit, elles accusent un retard de 16 ans par rapport à leurs homologues américaines.

Même si le coût total des cybercrimes commis mondialement a été évalué à plus de 1 T$ en 2018[9], le taux de détection de ces délits demeure très faible. En moyenne, il s'écoule 191 jours avant que l'on remarque une atteinte à la sécurité, ce qui est inacceptable, car pendant ce temps, les victimes ne peuvent rien faire pour se protéger. Les entreprises canadiennes doivent maintenant exercer une surveillance pour détecter les incidents de sécurité le plus tôt possible et y remédier promptement. Voici quelques exemples de moyens de détection :

1. **Fournisseurs de services de sécurité gérés**
   La plupart des entreprises de soutien informatique proposent aujourd'hui des services professionnels de surveillance du matériel réseau, des appareils et des applications afin d'en assurer la sécurité. Les petits et grands fournisseurs de services de sécurité gérés peuvent aider ou même remplacer le service des TI de l'organisation. En externalisant ces tâches, il est possible de libérer des ressources internes afin qu'elles se concentrent sur les activités courantes.

2. **Pare-feu intelligents**
   Souvent intégrés aux routeurs ou à d'autres composantes des réseaux, ces dispositifs conviennent bien aux petites entreprises. Ils leur permettent d'être avisées en temps réel de toute atteinte à la sécurité ou de consulter les registres d'accès après une attaque. Plus intelligents que jamais, ils détectent les intrusions (au lieu de bloquer le trafic réseau provenant de sources indésirables), puis localisent et consignent les atteintes à la sécurité avec bien plus de précision qu'auparavant. Pour protéger efficacement les actifs de l'entreprise, les pare-feu doivent toutefois être mis à jour, configurés et surveillés correctement. Pour obtenir une meilleure protection, les petites et moyennes entreprises (PME) devraient se procurer des pare-feu comprenant des fonctions intégrées de détection et de prévention des intrusions.

3. **Antivirus préventifs**
   Tous les antivirus actuels analysent continuellement la mémoire des ordinateurs pour trouver des logiciels malveillants et les éliminer automatiquement. Ceux de marques établies (Norton, McAfee, F-Secure) permettent d'exercer un contrôle centralisé et d'avoir une vue d'ensemble du réseau de l'entreprise. Ainsi, même les PME ont la possibilité de gérer leur sécurité de manière centralisée. Les outils les plus répandus sur le marché offrent aussi une protection contre les rançongiciels, les enregistreurs de frappe et les dissimulateurs d'activité afin de prévenir et de détecter certaines des infections

9 www.cybintsolutions.com/cyber-security-facts-stats/

qui, de nos jours, sont les plus dommageables pour les entreprises. Puisqu'il est estimé que 10 millions de nouveaux logiciels malveillants se retrouvent sur Internet chaque mois[10], les entreprises ont besoin de toute l'aide qu'elles peuvent obtenir.

Selon 56 % des décideurs en matière de TI, l'hameçonnage ciblé est la principale menace à la sécurité, en particulier lorsqu'on sait que 92 % des logiciels malveillants sont transmis par courriel[11]. La priorité est donc accordée à la sécurité des courriels, au filtrage des pourriels et à la détection des logiciels malveillants pour tous les messages électroniques (y compris le clavardage).

Avis et signalement

Même si, sur le plan technique, la détection représente le plus grand défi pour les entreprises canadiennes, c'est la décision d'aviser ou non une personne d'une atteinte à la sécurité – en fonction du critère de « risque réel de préjudice grave » – qui constitue la principale difficulté de la direction. Celle-ci est en effet responsable d'apprécier les conséquences d'une atteinte à la sécurité et de prendre les mesures appropriées : aviser les victimes potentielles, faire un signalement au commissaire à la protection de la vie privée ou simplement sécuriser les systèmes de l'entreprise (si le risque est minime).

Risques et contre-mesures appropriées

Risques (ce qui pourrait mal aller)	Contre-mesures (stratégies d'atténuation et de protection)
RISQUES INTERNES OU LIÉS AU LIEU DE TRAVAIL	
• Les télétravailleurs sont plus vulnérables au piratage, parce qu'ils se connectent dans divers environnements. • Les employés peuvent introduire, au moyen d'un appareil mobile, des logiciels malveillants dans l'environnement de l'entreprise. • La perte d'un appareil mobile peut causer une grave atteinte à la sécurité des données qui doit être signalée et qui peut être embarrassante si elle est rendue publique. • Les appareils personnels pourraient ne pas respecter les normes de l'organisation.	• Offrir un accès sécurisé aux données et aux systèmes de l'entreprise au moyen d'un RPV, de canaux chiffrés et d'environnements virtuels, comme ceux qu'offrent VMware et Citrix. • Veiller à ce que seuls les appareils autorisés puissent se connecter au réseau de l'entreprise et à ce qu'ils soient automatiquement analysés au moment de la connexion. • Mettre en place des procédures pour désactiver l'utilisation et la suppression de données à partir d'appareils mobiles perdus ou volés. • Établir des politiques décrivant les comportements attendus et les conséquences de tout écart. • Compartimenter ou cloisonner les applications de l'entreprise pour les séparer des applications d'utilisateur et des données.

10 Statistiques sur les logiciels malveillants de AV-TEST pour juin 2019. www.av-test.org/en/statistics/malware/

11 Selon un article sur les faits saillants de 2018 en matière de cybersécurité. www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Risques (ce qui pourrait mal aller)	Contre-mesures (stratégies d'atténuation et de protection)
LOGICIELS MALVEILLANTS ET PRISES DE CONTRÔLE DE COMPTES	
• Les employés peuvent accidentellement télécharger et installer des logiciels malveillants. • Il peut arriver que les employés donnent leurs justificatifs d'identité en réponse à un courriel frauduleux. • En cliquant sur un hyperlien dans une page Web ou un courriel, les employés peuvent se retrouver sur un site conçu pour exploiter les failles du navigateur et installer un logiciel malveillant.	• Veiller à filtrer tous les téléchargements et toutes les activités sur le Web aux fins de sécurité. • Bloquer l'accès Internet aux sites malveillants connus (attaques, hameçonnage, etc.), et utiliser un filtrage par modèle pour identifier les sites inconnus et les activités inhabituelles effectuées par les applications installées. • Restreindre les droits des utilisateurs d'installer ou de mettre à jour des logiciels.
SÉCURITÉ DU RÉSEAU ET CONTRÔLE DES ACCÈS	
• Il peut y avoir des accès à distance inexpliqués. • L'activité du réseau et le trafic élevé peuvent être inhabituels. • On peut constater des anomalies dans les communications Web, la résolution DNS et les chaînes de l'agent utilisateur.	• Pour assurer la sécurité du réseau, tester et installer les mises à jour fournies par tous les fournisseurs de logiciels. • Effectuer régulièrement des tests d'intrusion. • Enquêter sur les hôtes tentant d'établir un canal de communication au moyen de requêtes DNS à des serveurs DNS inconnus, essayant de se connecter directement plutôt qu'en ayant recours à un serveur mandataire de l'entreprise, ou utilisant des chaînes d'agent utilisateur inhabituelles, comme celles qui incluent le nom d'hôte interne, car il peut s'agir de signes précurseurs d'une menace persistante.

Conclusion

La cybersécurité et la protection des données sont importantes pour toutes les entreprises, de la plus petite à la plus grande, car les cyberattaques peuvent les exposer à de lourdes pénalités financières et nuire à leur réputation. Il est donc recommandé d'offrir aux employés des programmes de formation standardisés sur la cybersécurité, afin de les aider à mieux détecter et prévenir les atteintes à la sécurité dans tous les aspects de leur travail. De plus, cela renforcera l'efficacité des contre-mesures en matière de cybersécurité et atténuera les risques à l'échelle de l'entreprise.

Le tableau des principaux risques et stratégies de cybersécurité présenté précédemment constitue un excellent aide-mémoire, en particulier pour les PME et les professionnels comptables. Comme complément d'information, nous vous suggérons de consulter les publications de CPA Canada et de l'AICPA, dont le cadre d'information SOC for Cybersecurity. Il existe en outre une foule de ressources sur les pratiques exemplaires normalisées du secteur (voir entre autres les contrôles de sécurité essentiels du CIS, le cadre de cybersécurité du NIST et les pratiques en matière de gestion de la sécurité d'ITIL), qui sont conformes à la norme ISO 27001 et aux objectifs de contrôle du cadre COBIT (Control Objectives for Information and Related Technology) de l'ISACA.

La présente publication s'inscrit dans la **série Tendance technologique**, qui porte sur les grandes tendances du domaine touchant le milieu comptable. Les documents de cette série sont disponibles sur notre site Web.