ASSURER LA PÉRENNITÉ

Dans le présent numéro

- Rapport sur l'état de l'industrie
- Les petites entreprises peuvent en faire plus pour former leurs employés sur la sécurité de l'information
- Tour d'horizon des questions relatives aux brèches de données
- Relation avec les clients

Rapport sur l'état de l'industrie

La protection des renseignements personnels et les atteintes à la sécurité des données continuent de faire les manchettes des grands journaux, révélant que des entreprises, peu importe leur taille, sont victimes de crimes malveillants ou d'erreurs regrettables. Dans un souci de protéger les informations confidentielles de leurs employés, de leurs clients et de leur entreprise, les dirigeants d'entreprises ne considèrent plus les politiques et procédures en matière de sécurité de l'information comme des mesures « accessoires », mais bien « essentielles ».

À mesure que de nouvelles menaces à la sécurité des données apparaissent, les gouvernements révisent et élaborent de nouvelles lois afin de protéger les renseignements personnels. Avec tous ces changements, les organisations peuvent avoir du mal à respecter les exigences en matière de sécurité de l'information, particulièrement dans les secteurs très réglementés, comme la santé et les services financiers, où les exigences liées à la protection des renseignements personnels sont extrêmement rigoureuses.

Alors que le sondage Shred-it 2015 sur la sécurité de l'information (*Information Security Tracker*) démontre que de plus en plus d'organisations sont au courant des obligations et des exigences en matière de protection des données, il révèle également que la connaissance ne se traduit pas automatiquement par la prise de mesures concrètes.

ASSURER LA PÉRENNITÉ

Selon le sondage sur la sécurité de l'information, 96 % des cadres supérieurs et 82 % des propriétaires de petites entreprises connaissent les exigences juridiques applicables à leur industrie en matière d'entreposage, de conservation et d'élimination des données confidentielles. Cependant, un pourcentage affligeant de 37 % des propriétaires de petites entreprises indiquent n'avoir aucun protocole en place pour la destruction sûre des informations confidentielles. L'écart entre les grandes et les petites entreprises est encore plus grand en ce qui a trait aux politiques sur la cybersécurité : 82 % des cadres supérieurs affirment avoir de telles politiques contre un maigre 31 % chez les propriétaires de petites entreprises.

Sans politiques ni protocoles adéquats en place en matière de sécurité de l'information, les organisations mettent en danger les informations personnelles et confidentielles de leurs clients et de leurs employés et courent également davantage de risques d'essuyer des pertes financières, de voir leur réputation entachée et d'avoir à faire face à des problèmes d'ordre juridique. Voilà pourquoi il est important pour les organisations d'élaborer des politiques globales qui tiennent compte des exigences législatives et qui visent la protection des données confidentielles à toutes les étapes de leur vie utile, de la collecte à la destruction, en passant par l'entreposage.

Si vous souhaitez connaître les points de vue actuels en matière de sécurité, les facteurs de risque et les stratégies de prévention contenus dans le Rapport sur l'état de l'industrie de cette année, visitez le Centre de ressources de Shred-it et téléchargez le rapport complet.

Les petites entreprises peuvent en faire plus pour former leurs employés sur la sécurité de l'information

Les politiques et procédures en matière de sécurité de l'information jouent un rôle important dans la protection des petites entreprises contre les atteintes à la protection des données. Toutefois, de nombreuses petites entreprises sapent leurs efforts en ne formant pas adéquatement leurs employés. Selon le sondage Shred-it 2015 sur la sécurité de l'information (*Information Security Tracker*), 69 % des petites entreprises n'offrent aucune formation à leurs employés sur les procédures en matière de sécurité de l'information ou le font uniquement de façon ponctuelle.

Nombre de petites entreprises peuvent négliger l'élaboration de protocoles sur la sécurité de l'information et la formation des employés en raison de leurs ressources limitées. Cependant, l'exposition au risque d'une atteinte à la protection des données peut s'avérer beaucoup plus coûteuse à long terme. Selon le *Ponemon Institute*, le coût moyen de la perte ou du vol d'un document est 250 $[1]. De plus, ce même rapport indique que, parmi les pays où l'étude a été menée, le nombre de bris de sécurité découlant d'une erreur humaine est plus élevé au Canada. De toute évidence, la formation des employés est un investissement qui rapporte à long terme.

Il est important que les petites entreprises se rendent compte que chacune des mesures qu'elles prennent pour améliorer leurs protocoles sur la sécurité de l'information et la formation de leurs employés est utile, qu'il s'agisse de demander aux employés de déchiqueter les documents dont ils n'ont plus besoin ou de rendre obligatoire le chiffrement des dispositifs mobiles. Lorsque l'on donne aux employés les connaissances requises, on contribue à protéger son entreprise de la fraude.

Shred-it aide les propriétaires de petites entreprises en leur offrant des conseils pratiques et réalisables destinés à leurs employés. Pour télécharger le document *Helpful Reminders* de Shred-it, veuillez visiter le Centre de ressources de Shred-it :

- Postes d'impression : les documents confidentiels laissés aux postes d'impression sont susceptibles d'être vus par des personnes malintentionnées, augmentant ainsi les risques d'une atteinte à la sécurité. Rappelez à vos employés de se demander « Ai-je tous les documents que j'ai imprimés? »
- Les bacs non sécurisés : Jeter des renseignements dans des bacs non sécurisés augmente le risque de fraude. Déchiqueter tous les documents de manière sûre élimine les doutes et n'empêche pas le recyclage de votre papier. Rappelez à vos employés : « Stop! Ce document doit être déchiqueté. »

ASSURER
LA PÉRENNITÉ

- Matériel inutilisé : Détruire de manière sûre tous les appareils obsolètes est la seule façon de garantir que les données qu'ils contiennent ne seront jamais récupérées. Rappelez à vos employés : « Ne faites pas que supprimer; détruisez! »
- Entreposage : Le verrouillage des unités de rangement et des classeurs protège contre les accès non autorisés aux renseignements confidentiels et aide à réduire le risque de fraude. Rappelez à vos employés : « Pensez à mettre sous clé les renseignements confidentiels. »

Tour d'horizon des questions relatives aux brèches de données

Dans chaque numéro, nous présentons un enjeu rattaché à la sécurité de l'information dont on entend beaucoup parler afin que les entreprises sachent comment elles peuvent atténuer des risques semblables.

Pour le présent trimestre, nous attirons l'attention sur un récent rapport publié par la commissaire à la protection de la vie privée de la Colombie-Britannique.

Rapport de la commissaire à la protection de la vie privée de la Colombie-Britannique. La commissaire à la protection de la vie privée de la C.-B., madame Elizabeth Denham, a procédé récemment à un examen approfondi de l'efficacité de la gestion des bris de la sécurité des données au sein des régies de la santé de la Colombie-Britannique. L'évaluation, effectuée d'avril à juin 2015, révèle que, parmi les bris de la sécurité des données les plus courants dont sont victimes les régies de la santé, on compte les communications envoyées aux mauvais destinataires, les erreurs humaines, la perte de dossiers, l'entreposage non sécurisé et les accès inappropriés.

Au cours de l'évaluation, la moitié des régies de la santé interrogées ont indiqué que malgré les politiques exigeant le recours à des boîtes d'entreposage verrouillées ou stipulant qu'aucun dossier physique ne doit être sorti, il y a encore des travailleurs de soins à domicile qui laissent des dossiers de patients dans des véhicules non verrouillés. De plus, le rapport révèle que les bris de la sécurité des données liés au vol ou à la perte de dispositifs portables non chiffrés, comme les ordinateurs portatifs ou les clés USB, continuent à être un problème, malgré les politiques obligeant le chiffrement de tous les dispositifs portables.

Par conséquent, madame Denham demande que des mesures immédiates soient prises par les régies de la santé provinciales afin de renforcer la protection des informations personnelles sur la santé des citoyens.

Ce que vous pouvez faire : La gestion des atteintes à la protection de la vie privée est un élément essentiel de tout programme de gestion global des atteintes à la protection de la vie privée. Même si de nombreuses régies de la santé appliquent des procédures rigoureuses en matière de sécurité de l'information, des améliorations sont encore nécessaires quant à l'entreposage et à la destruction sécuritaires des dossiers médicaux confidentiels. Il existe des mesures simples que les entreprises peuvent adopter afin de réduire les risques d'atteinte à la sécurité des données et de protéger les renseignements personnels des patients.

1) Fournir des boîtes avec serrure aux employés qui doivent transporter des dossiers de patients.
2) Avoir des protocoles clairs pour l'élimination des informations qui ne sont plus nécessaires et des dispositifs électroniques de stockages de données qu'on n'utilise plus.
3) Veiller à ce que les employés n'emportent les dispositifs portables hors du bureau que lorsque cela est nécessaire et s'assurer que ces dispositifs sont chiffrés.
4) N'autoriser personne à laisser des documents non sécurisés sur son bureau et mettre en place une politique exigeant le déchiquetage de tous les documents qui ne servent plus.
5) Instaurer une formation obligatoire et des formations de mise à jour sur les politiques et procédures en matière de sécurité de l'information.
6) Réviser régulièrement les politiques et procédures en matière de sécurité de l'information afin de s'assurer qu'elles respectent toujours les lois sur la protection des renseignements personnels.

ASSURER
LA PÉRENNITÉ

Relation avec les clients

C'est avec ses clients que Shred-it entretient ses relations les plus importantes; voilà pourquoi les partenaires de Shred-it ont suivi une formation pour offrir un service à la clientèle et un savoir-faire de haut niveau. Dans chaque numéro du bulletin, nous présentons un partenaire de Shred-it qui s'est surpassé pour offrir un service à la clientèle exceptionnel.

Wei Wen Bi, PCSI
RSC, Toronto Est

Partenaire de Shred-it depuis 2009, Wei Wen Bi est le parfait exemple de l'engagement de Shred-it à considérer l'expérience client du point de vue du client. Monsieur Bi souligne que pour lui, son travail consiste à toujours donner le meilleur à ses clients et à tenter de percevoir leurs préoccupations avant même qu'ils ne les expriment. Au travail, il est patient et a une bonne capacité de communication : une simple conversation est un excellent moyen de découvrir ce qui préoccupe le client pour ainsi être en mesure de voir avec lui comment Shred-it peut l'aider.

Le dévouement de Wei Wen se reflète dans l'excellence des relations qu'il entretient avec ses clients et dans l'appréciation continue que ceux-ci manifestent à l'égard de son service.

> *« Je tiens simplement à vous dire à quel point nous apprécions le service de Wei Wen Bi, notre RSC. Chaque fois qu'il vient à nos bureaux pour collecter nos documents à déchiqueter, il est très minutieux, poli et efficace, et surtout, c'est un plaisir de faire affaire avec lui. Je veux remercier Wei pour son excellent travail! »*
>
> — Sharon Hagerty, Toyota on the Park

Shred-it tient à féliciter Wei Wen Bi pour le professionnalisme et l'efficacité dont il fait preuve chaque fois qu'il sert un client, ainsi que pour son engagement continu à être un partenaire solide et fiable en matière de sécurité de l'information.

Pour d'autres renseignements au sujet de la sécurité de l'information, nous vous invitons à consulter le Centre de ressources de Shred-it : shredit.com/centre-de-resources.

Vous pouvez également demeurer informé en consultant les pages Facebook et LinkedIn de Shred-it ou nous suivre sur Twitter à @Shredit.

1. Rapport 2015 sur le coût des atteintes à la sécurité des données : Canada, page 1 – Ponemon Institute