ASSURER LA PÉRENNITÉ

Dans le présent numéro

Nous ne sommes pas encore numériques

Dans le milieu des affaires d'aujourd'hui, la majorité des organisations ne sont pas « sans papier »; chaque année, les Canadiens utilisent toujours, en moyenne, six millions de tonnes de papier[1]. Puisque le papier demeure une composante essentielle de la vie au travail, tous les bureaux comptent encore un bon nombre de disques durs, d'imprimantes, de télécopieurs, de photocopieurs et d'autres appareils semblables.

Malheureusement, les organisations ne réalisent pas toujours que ces appareils stockent de l'information confidentielle dans leurs disques durs; par conséquent, ils ne prennent pas les précautions nécessaires lorsqu'ils s'en débarrassent. Selon le sondage de Shred-it sur la sécurité 2014, 42 % des entreprises canadiennes interrogées n'ont jamais détruit leurs disques durs, clés USB ou autre matériel contenant des renseignements confidentiels, ce qui signifie qu'une quantité importante de données potentiellement confidentielles risque de tomber entre de mauvaises mains .

Lorsque les disques durs sont inutilisés, la seule façon de s'assurer que les données stockées sont complètement supprimées de les détruire de façon sécuritaire en retirant et en détruisant le disque dur avant de jeter, de recycler ou de vendre l'appareil.

ASSURER
LA PÉRENNITÉ

Trois lignes directrices simples conçues pour sauvegarder des disques durs en milieu de travail :

1. Effectuer un nettoyage régulier des locaux d'entreposage et éviter le stockage de disques durs inutilisés.

2. Détruire tous les disques durs inutilisés en faisant appel à un fournisseur tiers qui possède une chaîne de garde sécurisée et qui confirme la destruction afin d'avoir l'esprit tranquille et d'assurer que les données ne tomberont pas entre les mains de fraudeurs.

3. Examiner régulièrement la politique en matière de sécurité de l'information de son organisation afin d'y inclure les nouveaux types de médias électroniques.

Influence de la génération « Y » sur le lieu de travail et la sécurité des données

De plus en plus, les « Y » constituent l'un des segments d'employés les plus influents et dominants en milieu de travail. Au Canada, les spécialistes prévoient qu'en 2028, 75 % de la main-d'œuvre sera composée de « Y »[3].

Les valeurs de cette génération étant bien différentes de celles de leurs prédécesseurs, les « Y » ont véritablement un penchant pour la technologie et la flexibilité, ce qui exige aux organisations d'adapter leurs politiques et leurs procédures. En ce qui concerne la protection des données, il s'agit d'assurer que les politiques tiennent compte de la dépendance croissante envers la technologie, tout en garantissant la sécurité de l'information confidentielle.

Même s'ils sont axés sur la technologie, les « Y » semblent faire fi de la sécurité des données et de la protection de leur information personnelle permettant de les identifier[4]. Du point de vue de l'organisation, il est crucial d'aborder cette insouciance relative à la sécurité en ligne et de l'atténuer en mettant en place à l'échelle de l'entreprise des politiques portant sur les applications pour téléphone intelligent et les appareils personnels utilisés dans le cadre du travail.

Près de 70 % des « Y » continuent à utiliser des applications personnelles au bureau comme source de soutient à leur travail[5]. Parmi ceux-ci, 60 % n'expriment aucune préoccupation au sujet de la sécurité de l'entreprise relativement à l'utilisation de ces applications personnelles. Si l'on considère que 25 % des employés adultes américains ont déjà été victimes de piratage sur un dispositif personnel, les employeurs devraient s'inquiéter de la présence de ces appareils au travail, surtout qu'ils ne semblent pas qu'ils soient utilisés selon de strictes lignes directrices sur la sécurité[6].

Pour obtenir des conseils sur l'élaboration d'une politique « BYOD ou apporter votre propre périphérique » ou sur la façon de stocker l'information confidentielle de façon sécuritaire, veuillez visiter le Centre de ressources Shred-it shredit.com/fr-ca/centre-de-resources. Vous pouvez également vous tenir informé en suivant Shred-it sur Facebook et LinkedIn ou Twitter à @Shredit.

ASSURER
LA PÉRENNITÉ

Synthèse sur l'atteinte à la sécurité de l'information

La première étape pour régler un problème consiste à reconnaître qu'il existe. Dans chaque numéro, nous présentons un cas d'atteinte à la sécurité des données d'envergure pour montrer aux entreprises la façon d'atténuer des risques semblables. Ce trimestre, nous voulions présenter une enquête actuellement en cours à Terre-Neuve–et–Labrador.

Central Health (Terre-Neuve–et–Labrador) :
Une autorité sanitaire de Terre-Neuve–et–Labrador fait enquête sur une atteinte à la sécurité des données confidentielles après qu'un document contenant des renseignements de patients eut été pris dans un hôpital de Grand Falls-Windsor au début du mois de mais 2015[7]. Selon Rosemarie Goodyear, directrice générale de Central Health, le document, qui devait être éliminé à la fin du quart de travail des employés, était un rapport quotidien sur les patients assignés à un fournisseur de soins de santé et contenait les renseignements personnels de 16 patients, y compris le nom, l'âge et le diagnostic.

Le document a plutôt été trouvé dans la communauté et remis à un bureau de presse local, ce qui a incité un journaliste à communiquer avec l'un des patients. Ce sont des patients qui ont informé l'autorité sanitaire de l'atteinte à la sécurité. À ce jour, les 16 patients ou leurs familles ont été informés.

Ce que vous pouvez faire : Il est évident que l'industrie des soins de santé a besoin d'améliorer la sécurité des dossiers médicaux confidentiels, et il existe des étapes simples qu'une entreprise peut entreprendre pour réduire le risque d'une atteinte à la sécurité des données.

1. Fournir des protocoles clairs pour l'élimination de l'information qui n'est plus nécessaire, ainsi que des dispositifs de stockage électronique inutilisés.
2. S'assurer que les employés n'emportent les appareils portables hors du bureau seulement que si cette mesure est nécessaire.
3. Éviter que les employés conservent des documents non sécurisés sur leur bureau, et mettre en place une politique prévoyant le déchiquetage de tous les documents inutilisés.

ASSURER
LA PÉRENNITÉ

Relation avec les clients

La relation la plus importante de Shred-it est celle qu'elle a avec ses clients. Voilà pourquoi les partenaires de Shred-it sont formés pour offrir un service et une expertise de premier niveau. Dans chacun des numéros de notre bulletin, nous présentons un partenaire de Shred-it qui s'est surpassé pour offrir un service à la clientèle exceptionnel.

Heather Nelson
Agente interne des ventes, Toronto-Est

Heather Nelson ne ménage pas ses efforts pour satisfaire les besoins de ses clients et aborde chaque appel qu'elle reçoit avec un niveau d'engagement inégalé. Elle rend à l'aise tous les clients, en discutant avec eux de la sécurité de l'information pour cibler leurs besoins et les renseigner sur toute la gamme de moyens par lesquels Shred-it peut contribuer à réduire les risques de fraude.

Heather remercie Shred-it et sa direction de lui avoir offert l'assurance et les connaissances dont elle a besoin pour accomplir son travail. « J'ai confiance dans l'information que je transmets aux clients, car je sais que notre entreprise offre l'expérience, la qualité du service à la clientèle et l'engagement envers la sécurité pour satisfaire tous les besoins. »

« Grâce au souci du détail de Heather, à ses compétences poussées en service à la clientèle et à son rire contagieux, ce processus a été agréable, aisé et sans anicroche. Heather a tenu toutes les promesses et a satisfait à toutes les attentes de l'entreprise. De nos jours, il est rare qu'un fournisseur de services tire une si grande fierté de son travail. Heather et Shred-it forment une équipe solide. »

Shred-it aimerait saluer Heather pour son travail de service à la clientèle exceptionnel.

Pour d'autres renseignements au sujet de la sécurité de l'information, nous vous invitons à consulter le Centre de ressource de Shred-it : shredit.com/fr-ca/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. ID2 Communications, *Facts About Paper and Paper Waste.*
2. Ipsos Reid, Sondage sur la sécurité 2014, *Fourth Annual Shred-It Security Tracker Reveals Canadian Businesses Continue to be Complacent About Information Security.*
3. *« Like it or Not, Millennials Will Change the Workplace » Financial Post, 16 septembre 2013*
4. *« Will Millennials Be the Death of Data Security »* DarkReading.com, 27 janvier 2015
5. *« Why Millennials Ignore Security Protocols at Work »* Adweek, 2014,
6. *« BYOD Infographic: For Security, It's Not a Pretty Picture »* Welivesecurity.com, 4 avril 2012
7. *« Newfoundland Patient Data Breach investigated » Metro, 8 mai 2015*