ASSURER LA PÉRENNITÉ

Dans le présent numéro

Les entreprises doivent éviter ces erreurs courantes

La première mesure à prendre pour améliorer la protection des renseignements consiste à mener une évaluation rigoureuse des points faibles de votre entreprise. Pourtant, selon les résultats du sondage Information Security Tracker réalisé en 2014 par Shred-it, **une entreprise sur quatre au Canada** n'a jamais vérifié les protocoles en place pour entreposer et éliminer les renseignements confidentiels.[1]

Examinez attentivement les procédures de protection des renseignements en place dans votre organisation pour relever toute lacune et pouvoir y remédier et agir concrètement pour atténuer le risque.

Voici les 10 erreurs les plus courantes que commettent les entreprises :

1. **Autoriser les poubelles et bacs à recyclage non sécurisés :** Jeter des documents contenant des renseignements dans une poubelle non sécurisée est tout aussi risqué que de les laisser sur une imprimante ou un bureau. En adoptant une politique de tout déchiquetage, on n'a plus à se demander si un document est confidentiel ou non et on s'assure que les employés ne jetteront pas de renseignements confidentiels dans des poubelles non sécurisées par inadvertance.

ASSURER
LA PÉRENNITÉ

2. **Permettre aux employés de laisser des documents sur leur bureau ou dans des classeurs non verrouillés :** Sans une politique claire concernant les documents qu'on peut laisser sur le bureau ou sans unités de stockage verrouillables pour que les employés puissent protéger les renseignements personnels, tout document papier est exposé aux regards indiscrets et au vol de données, en plus d'être accessible au personnel externe, comme les équipes de nettoyage et d'entretien des locaux.
3. **Imprimantes non sécurisées :** Dans de nombreux bureaux, on n'exige pas des employés qu'ils utilisent un code de sécurité pour pouvoir imprimer, ce qui signifie que des renseignements confidentiels sont souvent imprimés et laissés au poste d'impression. De plus, les entreprises négligent souvent de détruire physiquement le disque dur des imprimantes en fin de vie, sans se rendre compte que les renseignements qui ont été imprimés sont stockés dans la mémoire de l'imprimante.
4. **Permettre aux employés d'emporter des renseignements confidentiels du bureau :** Le travail devenant de plus en plus mobile, les gens apportent leur travail à la maison. C'est très pratique, mais les employés risquent de laisser des renseignements personnels dans des endroits non sécurisés. Les entreprises devraient demander aux employés d'apporter ou d'imprimer des renseignements confidentiels à l'extérieur des lieux de travail uniquement en cas d'absolue nécessité et leur apprendre comment éliminer ces documents en toute sécurité.
5. **Permettre aux employés d'utiliser des téléphones intelligents personnels sans passer en revue les mesures de sécurité :** Grâce aux téléphones intelligents, les employés peuvent travailler d'à peu près n'importe où. Par contre, ces téléphones constituent aussi un point d'accès supplémentaire à des renseignements potentiellement confidentiels. Si votre entreprise n'exige pas l'utilisation de mots de passe (au minimum) ou d'une méthode de cryptage dans le cadre de son plan de cybersécurité, le risque d'atteinte à la protection des données est accru.
6. **Mauvaise gestion des appareils de TI :** Les dispositifs de stockage électronique sont très utiles quand on ne peut accéder au réseau de l'entreprise, mais ils augmentent aussi le risque de fraude. Les entreprises peuvent réduire le risque de fraude en exigeant que les dispositifs de stockage soient enregistrés et en veillant à ce qu'ils soient détruits en toute sécurité lorsqu'ils ne sont plus utilisés.
7. **Utiliser des tableaux blancs pour les réunions sans les effacer :** Un milieu de travail axé sur la collaboration peut favoriser la productivité et la pensée novatrice. Par contre, l'information confidentielle laissée sur les tableaux blancs peut accroître les risques pour la sécurité de l'organisation, puisque l'information est laissée à la vue de tous dans des zones communes. Il importe d'inclure dans les politiques de sécurité le nettoyage des tableaux blancs pour éviter que l'information ne tombe entre de mauvaises mains.
8. **Permettre le partage des mots de passe des comptes communs sans établir de politiques de transition claires :** Il est utile pour les employés de partager un compte en ligne commun, et cela peut limiter le nombre de comptes utilisés. Par contre, le fait d'utiliser un mot de passe commun que plusieurs personnes connaissent accroît la vulnérabilité, surtout lorsqu'un employé quitte l'entreprise.
9. **Ne pas former les employés :** La meilleure politique de protection des renseignements est celle que les employés respectent. Si les employés ne comprennent pas comment appliquer une politique ou pourquoi ils doivent la suivre, cela ne sert à rien. En investissant du temps pour aider les employés à suivre les règles, l'entreprise investit réellement dans la sécurité.
10. **Passer en revue et évaluer les politiques existantes :** Les risques pour la sécurité de l'information changent au fur et à mesure que les organisations changent et croissent. De nombreux directeurs d'entreprises procèdent à l'évaluation des risques des nouveaux programmes dès le départ, mais il importe de revoir régulièrement les politiques et procédures de sécurité pour qu'elles répondent à la réalité d'une entreprise en perpétuelle évolution.

ASSURER
LA PÉRENNITÉ

Le petit livre noir de la fraude

Tous les ans, les Canadiens perdent des millions de dollars, victimes de fraude en ligne, par la poste, par porte-à-porte et par téléphone.[2] Ce type de fraude peut causer des dommages dévastateurs aux entreprises. Il importe de se tenir informé pour pouvoir reconnaître ces situations de fraude et en protéger les renseignements confidentiels.

Les petites entreprises sont souvent visées par une forme de fraude dans laquelle on essaie de les faire payer pour faire inscrire leur nom dans un répertoire qui n'existe pas, ou pour une publicité qui ne sera jamais publiée ou diffusée. L'organisation est bernée par une fausse soumission fondée sur une entrée réelle dans un autre répertoire ou une publicité déjà parue dans une autre publication.

Selon le Bureau de la concurrence du Canada, vous pouvez vous protéger en employant les moyens suivants :

- Veiller à ce que les employés qui traitent les factures ou répondent aux appels soient informés de ces fraudes.
- S'assurer que les biens ou services ont été commandés et livrés avant de payer une facture.
- Ne jamais donner de renseignements sur l'entreprise sans savoir à quoi servira cette information.
- Ne jamais accepter une proposition d'affaires au téléphone — demander une version de l'offre par écrit.
- Limiter le nombre d'employés ayant accès aux fonds de l'entreprise ou le pouvoir d'approuver des achats.

Pour de plus amples renseignements sur la façon de reconnaître les fraudes, rendez-vous sur le site Bureau de la concurrence et téléchargez le document Le petit livre noir de la fraude.

Violation des données

La première étape dans la résolution d'un problème, c'est d'en connaître l'existence. Dans chaque numéro, nous présenterons un cas grave de violation des données survenu récemment pour montrer aux entreprises comment elles peuvent atténuer les risques comparables auxquels elles sont exposées.

Voici le cas de Book2Park.com :

Book2Park.com est un service de réservation de stationnement en ligne pour les aéroports des États Unis. Selon les sources, l'entreprise semble avoir été la dernière victime d'un groupe de cybercriminels qui a volé plus de 100 millions de cartes de crédit et de débit chez Target et Home Depot. Book2park.com est le troisième service de stationnement en ligne à être victime de ce groupe depuis décembre 2014.

Ce que vous pouvez faire :

Le cybercrime demeure l'une des plus grandes menaces pour les entreprises, et pourtant, selon le 4e sondage annuel Shred-it Security Tracker, 60 percent des organisations canadiennes déclarent n'avoir adopté aucune politique de cybersécurité. Il est important que les dirigeants d'entreprises veillent à ce que la portée de leurs protocoles de protection de l'information englobe la cybersécurité et l'élimination des médias électroniques et des disques durs. Il ne suffit pas d'effacer un disque dur pour détruire les données. Il a été prouvé que la destruction physique du disque dur est le seul moyen cent pour cent sûr de détruire les données qui s'y trouvent.

ASSURER
LA PÉRENNITÉ

Relation avec les clients

La relation la plus importante de Shred-it est celle qu'elle entretient avec ses clients. C'est pourquoi les partenaires de Shred-it sont formés pour procurer aux clients le meilleur service qui soit et une expertise hors pair. Dans chaque numéro, nous soulignerons le travail d'un partenaire Shred-it qui est allé au-delà des attentes pour offrir au client un service exceptionnel.

Edward Gyasi
Responsable de la sécurité client, Est de Toronto

Pour Edward Gyasi, un responsable de la sécurité client ne se contente pas de détruire les documents en toute sécurité; il cherche des moyens d'aider les clients à mettre à jour ou à améliorer leurs pratiques générales en matière de protection de l'information.

Edward a fait preuve d'un tel professionnalisme en approchant chaque situation en ayant le client en tête. Qu'il détruise plus de documents que prévu ou apporte des bacs supplémentaires au cas où le client en ait besoin, Edward cherche à régler les problèmes des clients. Grâce à cette attitude proactive, Edward a pu à la fois résoudre les problèmes des clients de manière novatrice et leur offrir un service de qualité supérieure.

« Edward a sans contredit fourni un excellent service à la clientèle, aujourd'hui! Merci Edward! »

Shred-it tient à souligner l'excellent travail d'Edward, qui a dépassé les attentes des clients en contribuant activement à réduire leur degré d'exposition à la fraude.

Pour d'autres renseignements au sujet de la sécurité de l'information, nous nous invitons a 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 Ipsos Reid, 2014 Information Security Tracker
2 Bureau de la concurrence Canada, 2013, Le Petit Livre Noir de la Fraude