ASSURER LA PÉRENNITÉ

Dans le présent numéro

Les petites entreprises canadiennes ignorent les menaces pour la sécurité de l'information

Alors que l'on observe un changement positif dans les comportements par comparaison avec les années antérieures, le 5e sondage annuel de Shred-it sur la sécurité de l'information a révélé que les cadres supérieurs des entreprises ont non seulement reconnu la véritable menace que représentent les brèches de données, mais qu'ils ont également pris des mesures concrètes pour améliorer leurs politiques et procédures de sécurité. En revanche, les propriétaires de petites entreprises ont fait très peu de progrès dans la lutte contre les risques pour la sécurité de l'information alors que l'écart se creuse entre les grandes et les petites entreprises lorsqu'il est question de sécurité de l'information.

Par exemple, 65 % des cadres de direction affirment qu'ils disposent de protocoles pour entreposer et éliminer les données confidentielles et que tous les employés respectent à la lettre ces protocoles, ce qui représente une hausse par rapport au taux de 42 % obtenu en 2014. Par comparaison, moins de la moitié (47 %) des petites entreprises mentionnent qu'elles disposent de protocoles pour entreposer et éliminer les données confidentielles et que tous les employés respectent à la lettre ces protocoles, tandis que l'on obtient un taux consternant de 37 % d'entreprises qui n'ont mis en place aucun protocole.

ASSURER
LA PÉRENNITÉ

De plus, les grandes organisations sont de plus en plus exigeantes à l'endroit de leurs fournisseurs; elles insistent pour que ces derniers investissent eux aussi dans la sécurité de l'information. Dans les faits, 45 % des grandes organisations exigent que les fournisseurs disposent d'une politique sur la sécurité de l'information et 41 % demandent un plan d'intervention en cas d'atteinte à la sécurité.

Les propriétaires de petites entreprises doivent comprendre que, s'ils restent à la traîne par rapport aux entreprises plus grandes, ils s'exposeront de plus en plus non seulement aux vols, aux fraudes et à de graves répercussions sur leurs finances et leur réputation qui peuvent mener à la faillite, mais ils risquent également de perdre le droit de travailler avec les grandes organisations qui sélectionnent rigoureusement leurs fournisseurs.

Pour obtenir d'autres résultats tirés du sondage annuel de Shred-it sur la sécurité de l'information 2015, prière de visiter notre Centre de ressources.

Prédateurs en ligne et sécurité numérique

Quand les organisations renouvellent l'équipement informatique et les dispositifs d'entreposage numérique, elles sont confrontées à une problématique, soit décider de ce qu'il faut faire des vieux biens de TI. Il est important d'éliminer et de détruire adéquatement les dispositifs d'entreposage des disques durs non seulement pour assurer la sécurité des données confidentielles, mais aussi pour respecter les lois et les règlements en vigueur portant sur l'entreposage et l'élimination des renseignements médicaux personnels et des renseignements d'identification.

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) énonce des règles fondamentales quant à la façon dont le secteur privé recueille, utilise ou divulgue des renseignements personnels dans le cadre d'activités commerciales. En vertu de la LPRPDE, il faut éliminer les renseignements personnels en empêchant toute atteinte à la vie privée.

La LPRPDE stipule également que, avant de se débarrasser d'appareils électroniques comme des ordinateurs, des photocopieurs ou des téléphones cellulaires, les organisations doivent s'assurer que tous les renseignements personnels ont été physiquement éliminés du disque dur de l'appareil[1].

La façon la plus efficace de s'assurer que les données confidentielles contenues dans ces appareils sont complètement supprimées et qu'elles ne risquent pas de causer une atteinte à la vie privée est de détruire de façon sécuritaire le disque dur avant de le jeter.

Toutefois, le sondage annuel de Shred-it sur la sécurité de l'information 2015 a révélé que 40 % des entreprises canadiennes sondées n'ont jamais détruit de disques durs, de clés USB ou d'autres dispositifs informatiques contenant des données confidentielles[2]. Cela signifie qu'un grand nombre d'organisations mettent non seulement en jeu les données personnelles et confidentielles de leurs clients et employés, mais qu'elles défient également la LPRPDE.

Une brèche de données entraîne de nombreuses conséquences – pertes financières, atteinte à la réputation et incidence juridique. Il est essentiel que les organisations protègent les renseignements confidentiels en retirant et en détruisant les disques durs non utilisés.

Pour obtenir des lignes directrices simples sur la protection des disques durs en milieu de travail, prière de visiter le Centre de ressources de Shred-it.

Tour d'horizon des questions relatives aux brèches de données

Dans chaque numéro, nous présentons un enjeu rattaché à la sécurité de l'information qui est bien en vue afin que les entreprises sachent comment elles peuvent atténuer des risques semblables.

ASSURER
LA PÉRENNITÉ

Pour le présent trimestre, nous voulions traiter du Centre de la sécurité des télécommunications Canada.

Centre de la sécurité des télécommunications (CST) : Par suite d'une violation de la vie privée à l'interne, l'agence d'espionnage électronique du Canada a mis en place une formation obligatoire de sensibilisation à la protection des renseignements personnels pour tous les employés. Selon Greta Bossenmaier, chef du CST, des responsables de la sécurité ministérielle ont été avisés en juillet 2014 qu'un dossier contenant des renseignements personnels relatifs aux cotes de sécurité avait reçu par erreur une cote de consultation par le public. Une enquête interne a permis de déterminer que les renseignements personnels de nature délicate de cinq individus — soit quatre employés du CST et une personne du public — ont été compromis[3]. Par conséquent, en mars 2015, madame Bossenmaier a adopté une nouvelle politique sur les atteintes à la vie privée à l'échelon administratif et mis en place une formation obligatoire de sensibilisation à la protection des renseignements personnels à l'intention de tout le personnel.

Ce que vous devez faire : Si les employés ignorent les procédures qui conviennent pour la gestion et la destruction des renseignements confidentiels, l'organisation est exposée à un risque de fraude plus grand. Malheureusement, il arrive trop souvent que les organisations canadiennes font peu de cas de la vulnérabilité dans leur milieu de travail; selon le sondage annuel de Shred-it sur la sécurité de l'information 2015, 36 % des petites entreprises ne donnent jamais de formation à leurs employés sur les protocoles relatifs à la sécurité de l'information tandis que 29 % des organisations plus grandes le font seulement une fois par année.

Il est essentiel que non seulement tous les employés connaissent et comprennent les politiques et les procédures de sécurité de leur organisation, mais aussi qu'ils s'engagent réellement à les suivre correctement. Les dirigeants d'entreprises peuvent prendre des mesures concrètes pour s'assurer que tous leurs employés respectent leurs politiques et procédures de destruction de l'information :

- **Formation aux employés sur une base régulière :** Toutes les entreprises devraient planifier des activités de formation sur une base continue pour s'assurer que leurs employés connaissent bien les politiques et procédures les plus récentes en matière de gestion des documents.

- **Désignation d'un chef de la sécurité de l'information :** La désignation d'un chef de la sécurité de l'information, soit une personne responsable de la supervision de l'engagement de l'organisation à l'égard de la sécurité de l'information, contribue à réduire le coût rattaché à un bris de sécurité. De plus, cela favorise la mise en place d'une culture de sécurité au sein de l'organisation.

- **Désignation de responsables de groupes de pratique :** Tout secteur d'activité au sein d'une organisation possède de l'information qu'il faut entreposer en toute sécurité puis éliminer lorsqu'elle n'est plus nécessaire. Si l'on nomme un responsable de la sécurité de l'information dans chaque secteur d'activité, on s'assure ainsi que tous les employés comprennent et suivent les politiques.

- **Calendrier de conservation et de destruction :** Pour éviter les questions concernant la conservation et la destruction des documents, indiquez clairement sur tous les documents et dossiers ce qu'ils contiennent, pendant combien de temps ils doivent être conservés et à quel moment ils doivent être détruits.

- **Examen et évaluation des politiques existantes :** La meilleure façon d'améliorer la sécurité au sein d'une organisation est de mener des vérifications fréquentes pour s'assurer que les politiques et procédures permettent d'éliminer les menaces à mesure qu'elles apparaissent.

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 exceptionnelle.

Arnold Rubio, PCSI
RSC, Toronto

Partenaire de Shred-it depuis près de 10 ans, Arnold Rubio tient non seulement à aider ses clients à détruire leurs données confidentielles, mais aussi à mettre en œuvre des politiques et des procédures relatives à la sécurité de l'information. Il a démontré clairement qu'il avait cet engagement à cœur lors d'une visite de routine dans une succursale bancaire locale.

> *« Arnold Rubio a fait montre d'un haut niveau d'intégrité et a démontré que nos RSC mettent en pratique les valeurs de Shred-it. »*
>
> — Philip Moores, directeur des opérations, Shred-it, Toronto-Est

En vidant les cabinets pendant son quart de travail, Arnold a découvert que de l'argent s'était accidentellement retrouvé dans l'un des bacs verrouillés. Constatant qu'une erreur avait probablement été commise, Arnold a immédiatement avisé le directeur de succursale et s'est assuré que l'argent avait été rendu de façon sécuritaire. Arnold a aussi pris le temps d'aider le directeur de succursale à cibler l'origine du problème et a trouvé une solution pour éliminer le risque que de l'argent se retrouve à nouveau dans les cabinets. Le directeur de succursale a été impressionné par le professionnalisme et le respect de la confidentialité dont Arnold a fait preuve lorsqu'il a découvert l'argent et travaillé en collaboration avec l'équipe pour mettre en œuvre une nouvelle procédure dans l'avenir.

Shred-it tient à féliciter Arnold pour son professionnalisme, son intégrité et son engagement à l'égard de la sécurité de l'information.

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. Commissariat à la protection de la vie privée du Canada, 2015, *Trousse d'outils en matière de vie privée*
2. Business Wire, 2015, *Le 5e sondage annuel de Shred-it sur la sécurité de l'information révèle que les petites entreprises canadiennes ignorent les menaces pour la sécurité de l'information*
3. CTV News, 2015, *File Breach at Electronic Spy Agency Prompts Mandatory Privacy Training*