DOCUMENT D'INFORMATION

Les secteurs à risque courants

LE SAVIEZ-VOUS?

En 2017, une brèche de données moyenne touchait plus de 24 000 dossiers. [1]

Avec autant de documents exposés à des risques, les entreprises de toute l'Amérique du Nord doivent être conscientes de leurs secteurs vulnérables.

L'absence de politiques :

De nombreuses entreprises n'ont pas de programmes officiels de formation sur la sécurité de l'information, de politiques sur la cybersécurité, de plans d'intervention en cas d'incident ni de procédures de sauvegarde et de restauration. Cette absence de politiques les rend donc vulnérables à une brèche de données.

La négligence des employés :

Les employés négligents qui ne respectent pas les politiques et les procédures comme il se doit représentent le plus grand risque des organisations. Divulguer un mot de passe, emporter inutilement des renseignements confidentiels, laisser des renseignements sans surveillance dans un lieu public, ce sont tous des actes qui font courir des risques à une organisation.

Les tierces parties :

Les entreprises transmettent souvent beaucoup de renseignements confidentiels à des fournisseurs externes comme des agences de création, des cabinets d'analyse de données et des professionnels du domaine juridique. Avec un aussi grand nombre de données transmises, il est important de vérifier dans quelle mesure les fournisseurs externes protègent adéquatement leurs propres données.

Les initiés :

Les brèches de données surviennent souvent lorsque des utilisateurs privilégiés abusent de leurs droits en transférant frauduleusement de l'argent ou en utilisant des renseignements personnels d'un client pour voler son identité.

L'équipement obsolète :

Lorsque les entreprises acquièrent de nouvelles technologies ou de nouveaux systèmes ou logiciels, elles peuvent entreposer ou ne pas éliminer adéquatement leur vieux matériel, ce qui peut accroître le risque de brèche de données.

Les arnaques en ligne :

Les fraudeurs peuvent accéder à des renseignements personnels par l'entremise de courriels d'affaires dont le but est d'arnaquer l'entreprise. Ils peuvent également envoyer des courriels visant à convaincre l'utilisateur de télécharger un logiciel malveillant ou de se connecter à un système malveillant.

La numérisation :

Avec l'arrivée de l'internet des objets qui lie tous les appareils entre eux, comme les téléphones, les véhicules et les ordinateurs personnels, il est primordial de s'assurer que vous êtes connecté à un réseau sécurisé afin d'éviter d'être victime de fraude.

3 conseils pour protéger votre entreprise

Repérez tous les secteurs de risque potentiels.

Effectuez une inspection de vos bureaux. Signalez tous les risques que vous voyez et prenez des me-sures pour les atténuer. Cette inspection vous permettra de découvrir les points faibles de votre entre-prise et de renforcer votre stratégie en matière de sécurité de l'information afin de protéger vos données.

Mettez en place des politiques sur la sécurité des lieux de travail.

En établissant des politiques exhaustives, comme une politique de tout déchiquetage et une politique de bureau rangé, vous incitez vos employés à réfléchir avant d'agir lorsqu'ils sont au travail. Ils seront ainsi poussés à se conformer aux règles et à protéger vos données.

Créez une culture de sécurité totale.

En adoptant une approche descendante et en intégrant la sécurité de l'information dans l'ensemble de votre entreprise, vous ferez en sorte que la culture de sécurité totale fasse partie intégrante du quotidien de vos employés. Par le fait même, ceux-ci seront amenés à considérer d'un œil neuf la destruction sé-curitaire des renseignements confidentiels.

Sources:
1. 2017 Cost of Data Breach Study, Ponemon Institute, 2017

Pour en apprendre davantage sur la sécurité de l'information et sur les façons de protéger vos données :

1 800 697-4733 | shredit.com/fr-ca

Shred-it®

Shred-it® est une solution Stericycle.