

Cinq façons de renforcer vos politiques de protection des données

Le saviez-vous?

Parmi les cabinets juridiques qui ont été victimes d'un bris de la sécurité de l'information,

37 % ont rapporté une perte en ce qui a trait aux heures facturables.

28 % d'entre eux ont engagé des frais élevés pour rectifier la situation.

22 % d'entre eux ont indiqué que l'incident avait entraîné des coûts liés au remplacement du matériel informatique et des logiciels dans les bureaux.

Source: "Law Firm Data Breaches," National Law Review, 2017

Le domaine juridique se modernise et s'efforce d'améliorer l'expérience client au moyen d'outils numériques. Toutefois, il est vital que les pratiques de votre cabinet en matière de sécurité de l'information évoluent au même rythme. Pour protéger vos clients d'un bris de la sécurité des données, vos employés doivent comprendre comment recueillir, conserver, manipuler et détruire les renseignements confidentiels dans un environnement de plus en plus axé sur le numérique.

La vie privée des clients et la confidentialité sont des piliers de la profession juridique, mais vos employés peuvent tout de même faire des erreurs.



Nous protégeons ce qui compte.

 Shred-it®

Faites de vos employés des experts de la protection des données

1. Formation dès le début, puis de façon régulière.

N'attendez pas qu'un bris de la sécurité des données survienne pour commencer à former vos employés. Informez-les dès le début qu'il incombe à chacun au sein du cabinet - et donc à eux aussi - de protéger les données confidentielles. Outillez-les : donnez-leur des conseils pratiques et des exemples réels pour les aider à adopter de bonnes habitudes qui protégeront les données confidentielles.

2. Aucune tolérance pour la négligence.

Plus il y a d'employés dans un cabinet, plus le risque est grand que l'un d'eux ne fasse preuve de négligence à l'égard des données confidentielles, voire ne cause délibérément une brèche de données. Enseignez à vos employés comment repérer les comportements négligents, contraires à l'éthique ou malveillants et habilitez-les à prendre les mesures nécessaires s'ils considèrent que les données confidentielles des clients sont en danger.

3. La priorité : la sécurité à l'extérieur du bureau.

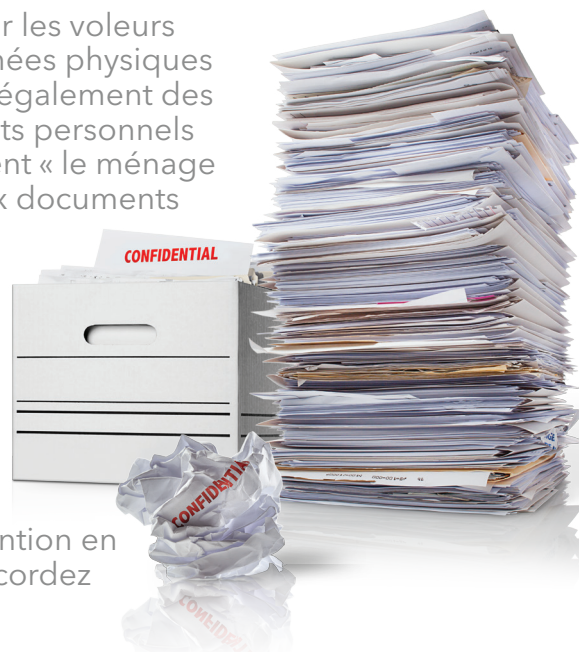
La perte ou le vol d'ordinateurs portatifs est l'une des causes les plus fréquentes de brèches de données dans les cabinets juridiques. Veillez à ce que votre cabinet soit doté d'une politique pour les employés mobiles ou travaillant à distance qui indique comment protéger les données lorsqu'on est en déplacement ou qu'on utilise un réseau non sécurisé. Adoptez également une politique de sécurité visant les employés qui utilisent leurs propres téléphones intelligents, ordinateurs portatifs ou tablettes pour le travail.

4. Souvenez-vous : « moins, c'est plus » (sécuritaire).

Les cabinets juridiques sont de véritables mines d'or pour les voleurs potentiels de données. Les cabinets possèdent des données physiques et numériques sur leurs clients et leurs entreprises, mais également des quantités potentiellement importantes de renseignements personnels sur les témoins dans les cas de litiges. Faites régulièrement « le ménage » afin d'entreposer et de détruire adéquatement les vieux documents papier et supports numériques contenant des données.

5. Soyez transparent.

Un cabinet juridique repose sur sa réputation. L'un des moyens les plus simples d'accroître votre réputation consiste à établir des protocoles simples et uniformes visant la manipulation de toutes les données des clients, confidentielles ou non. En expliquant, par exemple, vos protocoles de conservation des courriels et d'intervention en cas d'incident, vous démontrez à vos clients que vous accordez toujours la priorité à la sécurité de leurs renseignements.



Pour la tranquillité d'esprit, communiquez avec
Shred-it® dès aujourd'hui :
877-231-0634 | shredit.com/law

 Shred-it®