par
ERIC F.
GOSSELIN

Excusez-moi, j'ai perdu votre dossier…

Un de nos mandats auprès de nos clients est d'identifier, dans tous les aspects de leur vie financière, les failles de sécurité ou carrément les dangers qui peuvent les frapper à tout moment. On se doit alors de proposer des solutions, qu'elles soient sous forme d'acte notarié (testament, mandat de protection), d'assurance ou de produit d'investissement.

Notre pratique comporte aussi son lot de risques et on se doit de faire le même travail constant d'identification et de prévention. Dans le cas de la protection des renseignements personnels, c'est même une obligation déontologique.

Les experts identifient quatre facteurs menant à la perte d'information confidentielle : le piratage, un problème physique tel qu'un incendie ou une inondation, une défaillance technique (par exemple, un bris d'équipement informatique) et le facteur humain. Concentrons-nous sur le maillon faible de la chaîne de sécurité : le conseiller.

L'actualité est remplie d'histoires de pertes de données confidentielles dues au facteur humain. Pour s'en convaincre, on n'a qu'à penser à un certain ministre fédéral qui a oublié en 2008 un document de sécurité nationale chez sa copine… Rappelons-nous également Talvest, qui a perdu en 2006 un disque dur contenant l'information personnelle de 470 000 clients et, plus récemment, l'Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM), qui a égaré en 2013 un ordinateur portable contenant des renseignements sur 52 000 individus…

Heureusement, à part la honte accablant l'établissement fautif, aucune épidémie de vols d'identité n'a suivi, car les données avaient véritablement été perdues par accident; ce n'était pas le résultat d'un acte malveillant. Ce ne sera pas toujours le cas…

Que faire pour s'en protéger ?

Les premières précautions à prendre sont évidemment de nature physique. Il ne faut jamais laisser de dossiers dans un véhicule stationné, qu'ils soient sur support papier ou informatique. Un voleur désirant seulement la voiture pourrait voir sa journée aller encore mieux lorsqu'il obtiendra des informations lui permettant d'usurper facilement une identité et d'obtenir du crédit illégalement. Le coffre arrière n'est pas un coffre-fort, les données disparaissent avec le véhicule volé…

Comme vous ne faites pas garder vos enfants par un inconnu, au restaurant, vous ne demandez pas non plus à l'individu de la table d'à côté de surveiller vos affaires quelques minutes. C'est peut-être lui, le voleur. Je comprends qu'il n'est pas agréable de tout remballer et d'apporter ses dossiers aux toilettes, mais mieux vaut être prudent.

Résister aux pirates

Et pour les données informatiques ? Le risque zéro n'existe pas. Toutefois, vous pouvez poser certains gestes pour diminuer le risque lié à l'humain, particulièrement lors des déplacements.

Lorsque vous vous connectez à un réseau sans fil public (aéroport, restaurant, etc.), la précaution de base est d'utiliser un service de Virtual Private Network (VPN, ou réseau privé virtuel). Celui-ci brouille les données et votre emplacement, en faisant croire au réseau que vous êtes situé ailleurs dans le monde, ce qui vous rend moins intéressant et vulnérable aux yeux des pirates. Personnellement, j'utilise SurfEasy VPN, mais il y a des centaines d'entreprises qui offrent ce service pour environ dix dollars par mois.

Si vos informations sont sur une clé USB, un disque dur portatif ou un ordinateur portable, le minimum que vous devriez faire, en plus d'utiliser un mot de passe complexe pour y accéder, est d'encrypter les données. Ce processus rend le contenu incompréhensible à celui qui n'a pas la clé pour déchiffrer l'information.

Ici encore, une panoplie d'entreprises offrent des solutions, dont certaines gratuitement (mais je me méfie toujours lorsque c'est « gratuit », car l'usager en paie habituellement le prix autrement, par exemple en devenant sujet à des publicités ciblées) ou à des coûts fort variables en fonction des besoins de sécurité. Il existe BitLocker, de Microsoft, et FileVault 2, d'Apple, mais d'autres grands noms comme ESET, IObit ou Symantec offrent également de tels produits.

Cependant, rien de ce qui précède ne protège contre le bête oubli ou la simple perte de l'outil technologique. Ça arrive. Vous pouvez quand même dormir tranquille si vous avez activé les fonctions de traçabilité de votre appareil mobile permettant, entre autres, d'effacer à distance la totalité de son contenu.

Google offre le service pour les téléphones et tablettes de type Android et l'option est aussi simple à activer sur les produits Apple. Pour l'ordinateur portable Mac, la fonction est gratuite. Du côté de Windows, la compagnie Absolute LoJack offre, pour une vingtaine de dollars par année, de verrouiller à distance et d'effacer le contenu entier de l'appareil sur demande.

Vous n'avez rien fait de tout ça et avez perdu l'information personnelle d'un ou de plusieurs clients ? Vous devriez en aviser le service de conformité de votre entreprise, révéler le problème aux clients rapidement et tenir au courant votre assureur en responsabilité professionnelle et l'assureur entreprise de votre bureau, car certains avenants couvrent les frais juridiques découlant d'un tel évènement.

Comme il est toujours moins coûteux de prévenir que de guérir, je vous suggère de faire l'inventaire des risques que vous courez avec les données personnelles de vos clients et d'y opposer les protections pertinentes.

ERIC F. GOSSELIN, Adm.A., est planificateur financier, conseiller en sécurité financière et représentant en épargne collective rattaché aux Services en placements PEAK.