

## dossiers

# Technologies

## Sécurité de l'information

### Vos poubelles en disent beaucoup sur vous

**Vol d'identité.** Protéger les données de ses clients et de ses employés est une obligation légale de l'entreprise.

par Didier Bert > dossiers@transcontinental.ca

La profusion d'informations facilement accessibles fait la vie belle aux voleurs d'identité. « C'est un jeu d'enfant : l'information à notre sujet se retrouve partout », mentionne Jean-Sébastien Bilodeau, responsable de la sécurité chez Victrix, une firme montréalaise spécialisée en sécurité informatique.

Une équipe de Victrix est allée fouiller dans les poubelles, littéralement, d'une de ses entreprises-clientes, à sa demande évidemment. La récolte a été fructueuse : numéros de compte des employés et adresses. « Il aurait été très facile de se faire passer pour un employé de cette entreprise », note M. Bilodeau.

Les voleurs d'identité se servent de l'information confidentielle comme d'une clé pour accéder à d'autres informations ou pour commettre une fraude. Il est plus facile de trouver des renseignements personnels dans les poubelles ou bacs de recyclage que de se lancer dans le piratage sur

le Web. « Il faut être très malchanceux pour se faire voler son identité en ligne », rappelle M. Bilodeau.

#### La responsabilité de l'entreprise

L'entreprise doit réduire les risques en cette matière et éviter de laisser traîner des informations personnelles. Par exemple, elle peut demander à ne plus recevoir ses états de compte par courrier, optant pour le service en ligne, et limiter l'impression des documents sensibles.

Christian Lecompte, consultant en gestion des risques informationnels, suggère de s'interroger sur la pertinence de garder, ou non, ses factures d'affaires.

« Il est trop facile de récupérer des documents dans les bacs de recyclage des quartiers d'affaires », constate Jean-Sébastien Bilodeau. Cela peut être la photocopie d'une carte de crédit ou d'un relevé de compte jeté par un employé. « Ce genre de papiers doit être

**1** Nombre d'habitants de l'Amérique du Nord qui sont victimes d'un vol d'identité à toutes les minutes, selon le site de la Gendarmerie Royale du Canada.

décheté avant d'être recyclé », conseille M. Bilodeau.

« Le risque pour toute entreprise est d'être la source du vol d'identité, dit Guillaume Séguin, conseiller principal en sécurité des technologies de l'information chez Okio. Sa réputation pourrait en souffrir. »

L'entreprise a aussi une responsabilité juridique quant aux données confidentielles qu'elle possède. La Loi sur la protection des renseignements personnels et les documents électroniques oblige les entreprises à « préciser les fins auxquelles les renseignements personnels sont recueillis », indique le site Web du Com-

missaire à la protection de la vie privée du Canada. « L'entreprise doit vérifier si elle traite de l'information privée », conseille Daniel Gaudreau, vice-président chargé de la technologie et de l'exploitation d'Above Sécurité, établie à Boisbriand. Si oui, il faudra mettre à jour les technologies, les processus et les connaissances du personnel pour protéger cet actif de l'entreprise, préconise M. Gaudreau.

#### Les données sensibles

L'entreprise devrait s'assurer que les données confidentielles ne soient accessibles qu'aux employés qui en ont besoin dans leur travail, comme le personnel du service financier ou des ressources humaines.

Lors de l'envoi d'informations confidentielles, celles-ci devraient être chiffrées. « Qu'arrivera-t-il si on perd la liste des mauvaises créances transmise à une agence de recouvrement ? Que fera la personne qui trouve ce document ? » interroge M. Séguin.

Si le malfaiteur doit faire des efforts pour déchiffrer une base de données, il va plutôt essayer d'en attaquer une autre, non protégée donc plus accessible. « Chiffrer ses renseignements permet de rendre l'attaque plus coûteuse », note Guillaume Séguin. †

