par John Wunderlich

Y a-t-il eu préjudice?

Il est devenu plus facile de déterminer s'il y a lieu de notifier les employés et les clients lors d'une brèche dans les renseignements personnels.

Il existe deux points de vue opposés en matière de notification lors d'une brèche dans les renseignements personnels :

- Toutes les personnes et tous les organismes de réglementation concernés devraient être notifiés chaque fois que se produit une atteinte à la vie privée.
- Les exigences en matière de notification lors d'une brèche dans les renseignements personnels devraient être éliminées, et on ne devrait être indemnisé que lorsqu'il existe des preuves de la présence d'un réel préjudice financier causé par cette atteinte à la vie privée.

Bien que ces énoncés représentent les deux extrêmes en matière de notification de brèche, la plupart des organisations se situant entre ces deux extrêmes, les deux points de vue ont leurs mérites.

Le premier énoncé, qui mise sur la protection des renseignements personnels, est fondé sur le concept de la vie privée en tant que droit. Les employés qui traitent les données ont donc l'obligation de révéler toute brèche aux personnes concernées. Le second énoncé suppose qu'une brèche dans les renseignements personnels est inoffensive en soi. C'est pourquoi les personnes concernées doivent prouver qu'il y a eu un réel préjudice financier pour recevoir une indemnisation monétaire. Agir autrement constituerait une restriction déraisonnable à la conduite des affaires.

Pour le praticien de la paie, la question est donc la suivante : « Quelle est la position mitoyenne raisonnable entre ces deux extrêmes qui tienne compte des lois canadiennes, des pratiques exemplaires de RH/paie et des attentes des gestionnaires et des employés? » Tournons-nous vers une autorité compétente en la matière pour nous guider.

En 2010, un amendement à la *Personal Information Protection Act* (PIPA) (Loi sur la protection des renseignements personnels) de l'Alberta a ajouté une nouvelle responsabilité pour les organisations d'aviser le Commissaire à l'information et aux renseignements personnels en cas d'incident « de perte ou d'accès non autorisé ou de divulgation de renseignements personnels où toute personne raisonnable pourrait conclure qu'il existe un risque réel de préjudice important à la personne. » Cet amendement accorde également au Commissaire le pouvoir d'exiger des organisations qu'elles notifient les personnes qui courent ce risque réel de subir un préjudice important résultant d'un tel incident.

Depuis que l'amendement est entré en vigueur, plusieurs décisions[1] ont été rendues concernant la notification d'une

[1] http://www.oipc.ab.ca/pages/OIP/BreachNotificationDecisions.aspx (en anglais seulement)

brèche qui nous guident sur ce qui constitue une divulgation en cas de risque réel de préjudice important à une personne.[2]

BRÈCHE TOUCHANT LA PAIE

Dans cette cause, l'organisation qui utilisait un fournisseur externe de service de paie avait noté qu'une période de paie spéciale non autorisée avait été ajoutée à son système, ainsi que trois nouveaux employés, et qu'une tentative de transférer de l'argent dans les comptes de ces nouveaux employés avait avorté. Le fournisseur de service de paie externe a confirmé qu'on avait accédé à son système à l'aide d'information d'authentification provenant du gestionnaire de la comptabilité de l'organisation et que les données sur la paie entrées incluaient des renseignements financiers et démographiques. Ni l'organisation, ni son fournisseur de service de paie « ne pouvaient fournir un historique d'expertise sur la nature exacte des renseignements qui avaient été consultés et peut-être même copiés au cours de la période d'accès non autorisé au système de paie. »

Les mesures de sécurité du système avaient-elles fonctionné? D'une part, l'employé de la comptabilité qui avait examiné les comptes, soit la protection administrative, avait décelé l'anomalie. Dans le même ordre d'idée, les mesures techniques mises en place par le fournisseur de service de paie avaient empêché le transfert non autorisé des fonds. Conséquemment, en ce qui concerne la sécurité financière du système, il n'y avait aucun préjudice.

Par contre, le système étant incapable d'identifier quels renseignements pouvant être associés à une personne avaient été consultés ou copiés, il existait une défaillance fondamentale dans les mesures de contrôle touchant les renseignements personnels.

Le Commissaire a déclaré : « J'ai pris la décision qu'il existait un risque réel de préjudice important pour les personnes concernées en référence à cet incident. J'ai fondé ma décision sur le fait que les renseignements concernés pourraient être utilisés pour commettre un vol d'identité, ce qui constitue un préjudice important. Il n'existe aucun historique d'expertise qui puisse confirmer la nature des renseignements auxquels on a accédé et, compte tenu de la nature sensible des renseignements, la possibilité demeure que les renseignements du système de paie aient été consultés et copiés. »

Il est peut-être important pour les lecteurs de savoir que le rapport mentionnait le nom de l'organisation dont le système de paie avait subi une brèche, mais non celui du fournisseur de service de paie. On peut donc conclure que la responsabilité incombe toujours à l'organisation. Bien que la plupart des fournisseurs mettent en place des mesures de protection des renseignements personnels et de sécurité, il est important de se rappeler qu'en dernier ressort, c'est toujours l'organisation qui est responsable.

UNE LEÇON À RETENIR POUR L'ORGANISATION

L'enseignement que l'on peut tirer de cette situation est que la simple consultation des données de paie peut constituer une sérieuse atteinte à la vie privée. En d'autres mots, les affirmations alléguant que les données n'ont pas été modifiées ou copiées sont insuffisantes pour fournir l'assurance que les renseignements personnels sont protégés. Ce message doit être transmis à tous les praticiens de la paie et aux employés du service technique qui soutiennent les systèmes de paie.

Pour assurer la protection des renseignements personnels, l'accès aux systèmes de paie, et les données qu'ils contiennent, *doit* être restreint au nombre minimum de personnes nécessaires pour assurer la fonction de la paie. ■

John Wunderlich est un consultant en matière de renseignements personnels et de sécurité basé à Toronto. Pour plus de renseignements, veuillez consulter son site Internet mis à jour de façon discontinue à **http://compliance.wunderlich.ca** *(en anglais seulement).*

[2] **P2011-ND-008 : http://www.oipc.ab.ca/Downloads/documentloader.ashx?id=2812 (en anglais seulement)**