# La sécurité qui n’intéressait pas

Par Isabelle Lafont Mis en ligne le jeudi 10 mars 2011

**Isabelle Lafont est étudiante dans le cadre du cours DRT 6929-O.**

**Tous les mardis, l Identity Theft Resource Center** (« ITRC ») publie ses statistiques quant aux brèches dans les systèmes de sécurité d entreprises américaines Suvrant dans cinq domaines prédéterminés : les banques, les affaires, l éducation, le gouvernement et la santé.

Dans son dernier rapport, du 8 mars dernier, les statistiques de l ITRC indiquait que le secteur des affaires accuse le plus grand pourcentage (54.5%) de brèches dans les systèmes de sécurité depuis le début de l année 2011 : 42 brèches touchant 736 487dossiers d individus. Aucun des dossiers n était encrypté. Sur 42 entreprises, une seule avait protégé ses dossiers par l utilisation d un mot de passe.

Une mauvaise semaine direz-vous ? Non. En février dernier, Ponemon Institute (« Ponemon »), commandité par Cenzic et Barracuda Networks, rendait publique une étude intitulée State of web Application Security. Le sommaire exécutif souligne des statistiques quelques peu inquiétantes : 73% des entreprises ayant fait l objet de l étude ont été piratées au moins une fois au cours des deux dernières années et 88% d entre elles accordent moins d importance à la sécurité informationnelle qu à leur budget café (soit environ 30$ par employé par mois) !

Pourtant, nous aurions pu penser que le régime de divulgation obligatoire adopté par plusieurs États américains aurait eu pour effet d encourager (voire d obliger) les entreprises à faire de la sécurité informationnelle une priorité. En effet, depuis 2003, certains États américains ont décidé d obliger statutairement les entreprises privées à aviser leurs clients d une brèche dans leur système de sécurité afin, d une part, que ces derniers puissent prendre des mesures afin de mitiger leurs dommages, et d autre part, de responsabiliser les entreprises [1] . Les coûts reliés à la campagne d informations de leurs clients sont plutôt prohibitifs, sans compter la mauvaise publicité associée à la divulgation [2]. Les entreprises qui omettent de divulguer un incident peuvent faire l objet de peines statutaires [3].

L efficacité du régime de divulgation américain est encore mitigée. Certains auteurs prétendent notamment que la mauvaise publicité que la divulgation apporte aux entreprises les encourage au contraire à taire tout incident malencontreux, empêchant ainsi les victimes de mitiger leurs dommages [4 ] . Dans les cas où elles informent leurs clients, la campagne d information des entreprises est parfois peu efficace puisque leurs lettres d information trouvent directement le chemin de la corbeille sans même avoir été ouvertes (« enveloppe triviality »).

Dans une certaine mesure, les Américains peuvent se consoler en regardant ces statistiques qui leur permettent d identifier et de mesurer le problème. En d autres mots, il s agit d un premier pas vers l élaboration d une meilleure solution. Il est difficile d en dire autant pour le Québec.

Au Québec, à l heure actuelle, il y a peu de données chiffrées sur la sécurité informationnelle (voir les publications de la Chaire de recherche du Canada en sécurité, identité et technologies pour quelques statistiques). Sauf les quelques cas rapportés par dans les médias et les entreprises qui veulent bien se soumettre à des sondages, il est bien difficile de recenser le nombre d entreprises privées qui subissent des intrusions inopinées dans leurs systèmes de sécurité et leurs conséquences. Ceci découle en partie du fait qu il n existe aucune obligation de divulgation au Québec. Les organisations policières ne

recueillent pas de statistiques sur les comportements criminels non plus. Conséquemment, nous ignorons à quel point nos données personnelles sont ou non en sécurité.

Pourtant, il n y a qu à regarder de l autre côté de la frontière pour voir que la sécurité informationnelle est préoccupation sérieuse. Il serait fallacieux de croire que les données personnelles sont mieux protégées par les entreprises québécoises que les entreprises américaines. Même le Gouvernement du Canada a récemment été l’objet d’une cyberattaque ! Sans être alarmiste, il est grand temps de s intéresser à la sécurité informationnelle et d en parler en dollars, question d intéresser les gestionnaires.

C est ce qu a d ailleurs fait l Alberta qui, depuis le 1er mai 2010, oblige les entreprises privées à aviser l’Alberta’s Information and Privacy Commissioner des données personnelles qui sont perdues, qui font l objet d un accès non autorisé ou qui sont divulguées sans l autorisation de leur propriétaire [5] . Dans certains cas, le Commissaire peut exiger que l entreprise informe les individus visés par la brèche [6] . L avenir nous dira si le modèle albertain s avérera efficace. Le cas échéant, le Québec pourrait s en inspirer !

---

[1] 1.L. RODE , « Database security breach notifications statutes : does placing the responsibility on the true victim increase data security ? », 43 HOUS. L.REV. 1597, 1601, 1619 et suiv. (2006-2007)

[2] 2.Id.

[3] 3. Id.

[4] 4.P.M. SCHWARTZ et E. J. JANGER, « Notification of date security breaches », 105 MICH. L. REV. 913, 928, 930 (2007)

[5] 5. Personal Information Protection Act, S.A. 2003, c. P-6.5, art. 34.1.

[6] 6.Id.