LES MESURES VISANT À FAIRE RESPECTER LA RÉGLEMENTATION FONT RESSORTIR LA NÉCESSITÉ DE CRÉER UN CADRE DE GOUVERNANCE POUR LA SÉCURITÉ DES RENSEIGNEMENTS

08 février 2017

Les récentes mesures prises par les commissaires à la protection de la vie privée du Canada et de l'Australie pour faire respecter la réglementation fournissent d'importantes orientations relativement à la conformité aux lois sur la protection des renseignements personnels. Avant toute chose, les organisations doivent établir un cadre adéquat pour la gouvernance de la sécurité des renseignements afin que des pratiques, procédures et systèmes adéquats permettant de protéger les renseignements personnels soient établis, compris de façon uniforme et mis en œuvre de façon efficace.

Mesures visant à faire respecter la réglementation — Atteinte à la protection des données d'Ashley Madison

En 2015, le site Web de rencontres extraconjugales discrètes d'Ashley Madison exploité par Avid Life Media (« ALM ») a été victime d'une cyberattaque menée par des pirates qui ont publié les détails (notamment des renseignements personnels sensibles) d'environ 36 millions de comptes d'utilisateurs du site en question. L'atteinte à la protection des données a fait l'objet d'une enquête conjointe de la part des commissaires à la protection de la vie privée du Canada et de l'Australie, qui a amené la Federal Trade Commission (« FTC ») des États-Unis et certains États américains à intenter des poursuites.

En août 2016, les commissaires à la protection de la vie privée ont produit un rapport conjoint faisant état de leurs conclusions voulant qu'ALM ait enfreint plusieurs dispositions de la *Loi sur la protection des renseignements personnels et les documents* électroniques du Canada et de la *Privacy Act* de 1988 de l'Australie, et ont publié les ententes de règlement qu'ils ont conclues avec ALM. En décembre 2016, la FTC a annoncé qu'ALM avait accepté de régler les actions en justice qu'elle-même et certains États avaient intentées en payant 1,6 M$ et en se conformant à une ordonnance prescrite (*stipulated order*). Le rapport conjoint, les ententes de règlement et

l'ordonnance prescrite comportent d'importantes directives en matière de respect des lois sur la protection des renseignements personnels.

Rapport conjoint des commissaires à la protection de la vie privée

La législation canadienne sur la protection des renseignements personnels oblige les organisations à protéger la sécurité, la confidentialité et l'intégrité des renseignements personnels qu'elles détiennent en instaurant des mesures de sécurité (c.-à-d. des mesures techniques, des moyens matériels et des mesures administratives) qui sont adaptées à la sensibilité des renseignements d'après une évaluation raisonnable du risque financier, du risque d'atteinte à la réputation et d'autres risques qu'une atteinte à la sécurité des données peut poser selon le contexte.

Le rapport conjoint des commissaires précise que, à la lumière de la leçon tirée du piratage du site d'Ashley Madison « qui s'applique le plus largement, les organisations qui détiennent des renseignements personnels sous forme électronique doivent adopter des processus, des procédures et des systèmes explicites et appropriés afin de gérer les risques d'atteinte à la sécurité des données. Elles doivent également posséder l'expertise adéquate (interne ou externe) pour ce faire ». Le rapport conjoint énonce de plus que, « [d]ans le cas […] de toute organisation détenant de grandes quantités de renseignements personnels sensibles, il ne suffit pas de veiller à la sécurité des données; il faut également disposer d'un cadre de gouvernance adéquat et cohérent ».

Selon les ententes de règlement qu'elle a conclues avec les commissaires à la protection de la vie privée, ALM est tenue d'établir, de documenter et de mettre en œuvre un cadre de sécurité de l'information et des pratiques de sécurité de l'information appropriés. Pour en savoir davantage sur le rapport conjoint des commissaires à la protection de la vie privée, veuillez vous reporter au bulletin de BLG intitulé Atteinte à la sécurité des données dans l'affaire Ashley Madison : leçons à tirer et recommandations précieuses pour toutes les entreprises.

Actions en justice de la FTC et des États

Les poursuites intentées par la FTC et certains États américains contre ALM ont été réglées en tenant compte d'une ordonnance prescrite qui oblige cette dernière à établir, à mettre en œuvre et à maintenir un programme de sécurité de l'information exhaustif et dûment documenté, y compris des mesures techniques, des moyens matériels et des mesures administratives appropriés et raisonnablement conçus pour protéger la sécurité, la confidentialité et l'intégrité des renseignements personnels détenus par ALM. Le programme obligatoire doit comprendre les éléments suivants :

- La nomination d'un employé à qui incomberont la responsabilité et la coordination du programme de sécurité de l'information d'ALM.
- Le repérage et l'évaluation des risques internes et externes pour la sécurité, la confidentialité et l'intégrité des renseignements personnels dans chaque secteur d'activité d'ALM (p. ex., la formation et la gestion du personnel, les systèmes d'information et la prévention, la détection des incidents liés à la sécurité des données et les mesures prises en réaction à ceux-ci) ainsi que l'évaluation du caractère suffisant des mesures de sécurité existantes pour contrôler ces risques.

- La conception et la mise en œuvre de mesures de sécurité raisonnables pour contrôler les risques repérés ainsi que des tests et suivis réguliers pour en évaluer l'efficacité.
- L'élaboration et l'application de mesures raisonnables pour choisir et engager des fournisseurs de service capables d'assurer la sécurité des renseignements personnels qu'ALM leur transmet et obliger ceux-ci à mettre en place et à maintenir des mesures appropriées pour ce faire.
- L'évaluation et l'ajustement périodiques du programme de sécurité de l'information à la lumière des résultats des tests et suivis périodiques, des changements importants apportés aux activités ou aux ententes commerciales d'ALM, ou de toute autre circonstance connue pertinente.

L'ordonnance prescrite oblige aussi ALM à engager une tierce partie compétente et indépendante qui évaluera périodiquement le programme de sécurité de l'information de l'entreprise au cours des vingt prochaines années.

Commentaire

Un cadre de sécurité de l'information approprié et documenté aidera non seulement une organisation à respecter les lois sur la protection des renseignements personnels, mais il aidera celle-ci ainsi que ses dirigeants à se conformer aux autres responsabilités et obligations qui leur incombent aux yeux de la loi en ce qui a trait à la gestion des risques et à la protection de renseignements sensibles qui sont réglementés et protégés. Pour en savoir davantage sur ces responsabilités et obligations, veuillez consulter les bulletins de BLG suivants (en anglais seulement) : *Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*; *Regulatory Guidance from the Canadian Securities Administrators*; *Cybersecurity Guidance from Investment Industry Organization*; *PCI DSS Requirements for Incident Response Plan*; *Data Incident Notification Obligations*; *Guidance for Corporate Directors* et *Cyber-Risk Management Guidance from Financial Institution Regulators*.

Les commissaires à la protection de la vie privée, les autorités de réglementation et les organisations sectorielles ont publié des orientations utiles pour l'établissement d'un cadre de gouvernance de la sécurité de l'information qui repose sur des normes et des pratiques optimales acceptées par l'industrie. Voici, à titre d'exemples, des bulletins de BLG et autres publications sur le sujet : Bulletin d'interprétation : Mesures de sécurité; Bulletin d'interprétation : Responsabilité; *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*; Trousse d'outils en matière de vie privée – Guide à l'intention des entreprises et des organisations; Protéger les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations; *Start with Security – A Guide for Business*; *The NIST Cybersecurity Framework and the FTC*; *Conseils sur l'autoévaluation en matière de cybersécurité du BSIF*; *Guide des pratiques exemplaires en matière de cybersécurité de l'OCRCVM* et *Avis 11-332 du personnel des ACVM Cybersécurité*.

Par

Bradley Freedman

Services

Cybersécurité, respect de la vie privée et protection des renseignements personnels

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749