CLASSESAFFAIRES
ACTUALITÉS ▪ SÉMINAIRES ▪ PERSPECTIVES

Blakes

Cyberattaques : atténuer la responsabilité des administrateurs

Hélène Deschamps Marquis et Joe Abdul-Massih

Plusieurs anciens dirigeants de Yahoo! Inc. ont récemment réglé une action oblique (ou action dérivée) pour un montant de 29 M$ US, fondée sur des atteintes à la protection des données qui ont touché trois milliards de comptes en 2013 et 2014. À l'époque, ces atteintes à la protection des données constituaient la plus importante intrusion connue du réseau informatique d'une société. En l'absence de jurisprudence canadienne sur la responsabilité des administrateurs dans le contexte d'une atteinte à la protection des données, les administrateurs auraient intérêt à passer en revue la jurisprudence américaine en la matière, de même qu'à adapter leur stratégie et approche à l'égard de la confidentialité et de la sécurité des données.

LEÇONS TIRÉES DE L'ATTEINTE À LA PROTECTION DES DONNÉES DE YAHOO

En février 2017, les actionnaires de Yahoo! Inc. ont intenté une action oblique contre le conseil d'administration et des cadres supérieurs de Yahoo! Inc. devant la Cour de district des États-Unis pour le district nord de la Californie. La poursuite visait tout particulièrement la façon dont ces hauts dirigeants avaient géré les atteintes à la protection des données survenues en 2013 et 2014. Les actionnaires alléguaient que les hauts dirigeants de Yahoo! Inc. avaient manqué à leurs obligations fiduciaires en omettant de protéger les données de Yahoo! Inc. et de mettre en œuvre des mécanismes de sécurité adéquats pour prévenir les cyberattaques, ainsi qu'en diffusant de fausses déclarations à propos de la connaissance par Yahoo! Inc. de ces atteintes à la protection des données.

Après la divulgation des atteintes à la protection des données, Verizon, qui avait conclu une convention d'achat d'actions avec Yahoo! Inc. en 2016 relativement à la vente d'actifs d'exploitation de Yahoo! Inc., a rapidement réduit de 350 M$ US le prix d'achat qu'elle devait verser à Yahoo! Inc.

D'après certains commentateurs, cette affaire illustre une nouvelle tendance voulant que les administrateurs et les dirigeants soient de plus en plus tenus responsables à l'égard de leur conduite au cours d'une atteinte à la protection des données. D'autres attribuent plutôt ce règlement important à la capacité de Verizon de négocier une réduction considérable du prix d'achat. Contrairement à d'autres cas d'action oblique, les dommages subis par la société étaient faciles à quantifier.

RESPONSABILITÉS DES CONSEILS D'ADMINISTRATION AU CANADA

La *Loi canadienne sur les sociétés par actions* (la « LCSA ») et d'autres lois sur les sociétés comparables prévoient que chaque administrateur et dirigeant d'une société doit, dans l'exercice de ses fonctions, agir avec le soin, la diligence et la compétence dont ferait preuve, en pareilles circonstances, une personne raisonnablement prudente.

Dans leur interprétation de la conformité à cette norme, les tribunaux reconnaissent que les décisions d'affaires comportent habituellement un certain risque et qu'il ne serait donc pas approprié de juger a posteriori des décisions antérieures. Aux termes de la LCSA, un administrateur s'est acquitté de son obligation de diligence s'il s'est appuyé de bonne foi sur les rapports des personnes dont la profession permet d'accorder foi à leurs déclarations.

La prévention de toute atteinte à la sécurité des données est un objectif qui est certes louable, mais qui peut être impossible ou difficile à atteindre en raison de la complexité des systèmes informatiques et de l'ingéniosité dont font constamment preuve les cybercriminels. La responsabilité des administrateurs des sociétés canadiennes ne devrait donc pas être évaluée en fonction d'un tel objectif. Conformément à leur obligation de diligence, les membres du conseil d'administration devraient appliquer les normes de l'industrie en matière de surveillance des risques liés à la cybersécurité et réévaluer continuellement l'évolution desdites normes et des risques.

CONSEILS EN MATIÈRE DE GESTION DES RISQUES

D'après une étude récente présentant les coûts des atteintes à la protection des données dans 13 pays, le coût moyen d'une atteinte à la protection des données au Canada est de 5,78 M$ CA, et le coût moyen par information perdue ou volée est de 255 $ CA. Pour en savoir davantage, consultez notre infographie de juillet 2017 intitulée *Atteintes à la protection des données et coûts de la cybercriminalité au Canada*.

Un facteur qui contribue à réduire les coûts d'une atteinte à la protection des données est l'intervention du conseil d'administration à l'égard des questions relatives à la cybersécurité. Le conseil d'administration n'a pas besoin de se pencher sur les détails techniques relatifs à la cybersécurité, comme la réalisation de tests de pénétration ou la mise en place de pare-feu efficaces; il doit toutefois saisir les enjeux propres à la gestion des risques associés à la cybersécurité à l'échelle de l'entreprise, en plus de donner le ton en matière d'engagement à l'égard de la cybersécurité.

Voici quelques moyens par lesquels un conseil d'administration peut mettre à profit ses capacités d'analyse et de gestion des risques afin de surveiller et de renforcer la cybersécurité, d'atténuer sa responsabilité et de respecter ses obligations fiduciaires :

1. **Établir une structure de gestion de la protection de la vie privée** en s'assurant de mettre en place un agent de protection des renseignements personnels, une équipe chargée de la protection de l'information et une équipe d'intervention en cas d'incident, et veiller à ce que ceux-ci passent en revue les politiques, les procédures et les plans d'intervention en cas d'incident existants afin de cerner tout enjeu lié à la cybersécurité et à la protection des données.

2. **Effectuer un mappage des données** en examinant les types de renseignements personnels qui sont recueillis par une organisation, de même que les autres données névralgiques pour une organisation afin de s'assurer que les pratiques de gestion des données sont adéquates.

3. **Évaluer les systèmes d'information** en examinant les outils de sécurité se trouvant dans le réseau de l'organisation et les applications logicielles qui ont été installées.

4. **Passer en revue les pratiques de formation** pour veiller à ce que le personnel clé de l'organisation en matière de TI et de sécurité de l'information ait reçu une formation adéquate sur la gestion d'incidents et l'intervention en pareil cas.

5. **Mener périodiquement des exercices sur table et des simulations de cyberattaques** avec l'équipe d'intervention en cas d'incident et d'autres professionnels de l'organisation.

6. **Être proactif** en faisant appel à un conseiller juridique externe qui agira comme coach en matière d'atteintes à la protection des données afin de s'assurer que l'organisation est prête à faire face à celles-ci.

COORDONNÉES

Hélène Deschamps Marquis
helene.deschampsmarquis@blakes.com
514-982-4042

Joe Abdul-Massih
joe.abdul-massih@blakes.com
514-982-4297