INSTITUTIONS FINANCIÈRES : LES OBLIGATIONS ACCRUES DU BSIF EN MATIÈRE DE SIGNALEMENT DES INCIDENTS LIÉS À LA CYBERSÉCURITÉ SONT MAINTENANT EN VIGUEUR

Publié le 8 avril, 2019

Catégories: Perspectives, Publications

Le 24 janvier 2019, le Bureau du surintendant des institutions financières (le « **BSIF** ») a publié le préavis intitulé *Signalement des incidents liés à la technologie et à la cybersécurité*[1] (le « **Préavis** »), qui énonce les attentes du BSIF en ce qui concerne le signalement des incidents liés à la technologie et à la cybersécurité. Le Préavis, qui est entré en vigueur le 31 mars 2019, s'applique à toutes les institutions financières fédérales (les « **IFF** »).

Conformément au Préavis, les IFF sont tenues de signaler tout incident lié à la technologie ou à la cybersécurité qui « pourrait avoir des conséquences importantes sur les activités habituelles d'une IFF, y compris sur les plans de la confidentialité, de l'intégrité ou de la disponibilité de ses systèmes ou de ses renseignements ». Si une IFF estime que le niveau de gravité d'un incident est « élevé ou critique », elle doit aviser le BSIF le plus rapidement possible, et au plus tard 72 heures après avoir déterminé que l'incident devait être signalé. Pour en savoir plus sur le processus de signalement et sur ce qui le différencie des obligations de déclaration des atteintes aux mesures de sécurité prévues par la *Loi sur la protection des renseignements personnels et les documents électroniques* (la « **LPRPDE** »), voir notre publication récente, « Le BSIF intensifie ses efforts en matière de cybersécurité en publiant un nouveau préavis sur le signalement des incidents liés à la technologie et à la cybersécurité ».

Afin de s'assurer que les IFF se conforment aux dispositions du Préavis et aux attentes du BSIF, nous leur recommandons de prendre plusieurs mesures, dont les suivantes :

- adopter une approche en cascade afin de s'assurer que tous les membres de l'IFF, tant les membres de la direction et les membres du conseil que les employés, participent activement au programme de l'IFF en matière de cybersécurité et y adhèrent;
- effectuer périodiquement des évaluations du risque, des audits de sécurité et des vérifications diligentes à l'égard des fournisseurs et des travailleurs en sous-traitance lorsqu'elles concluent des ententes avec eux (et inclure des exigences écrites dans les contrats);
- désigner un administrateur du programme qui doit rendre compte à l'organisation;

- élaborer des politiques et des procédures écrites, y compris, et cela est essentiel, un plan d'intervention en cas d'incident, fondé sur ce qui est mentionné ci-dessus.

La vérification régulière des contrôles internes, l'offre de programmes de formation aux membres du personnel et la mise à jour des procédures de conformité rehausseront l'efficacité de ces recommandations.

Les organisations sont invitées à consulter le document de McMillan intitulé Services d'intervention d'urgence pour obtenir plus d'information, et à communiquer avec un des membres de notre équipe pour toutes autres questions.

par Darcy Ammerman, Ryan J. Black, Grace Shaw et Alex Tyzuk (étudiant en droit)

[1] Disponible sous Signalement des incidents liés à la technologie et à la cybersécurité.[ps2id id='1' target='/]

Mise en garde