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

Publié le 6 février, 2019

Catégories: Perspectives, Publications

Ce nouveau préavis à l'intention des institutions financières fédérales (les « **IFF** ») constitue une bonne nouvelle dans le contexte canadien de la cybersécurité en constante évolution.

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* (le « **Préavis** »), qui énonce les attentes du BSIF en matière de signalement des incidents liés à la technologie et à la cybersécurité. Le Préavis est un document complémentaire à la note d'information du BSFI intitulée *Conseils sur l'auto-évaluation en matière de cybersécurité* datant du mois d'octobre 2013 (les « **Conseils sur la cybersécurité** »), et doit être lu conjointement avec celle-ci. Le Préavis s'applique à toutes les IFF à compter du 31 mars 2019. D'ici là, les IFF doivent continuer de signaler les incidents majeurs selon les directives qui leur ont déjà été fournies à cet effet.

Le Préavis témoigne de l'attention que le BSIF porte continuellement à la technologie et à la cybersécurité, et s'inscrit dans le cadre de la campagne de sensibilisation plus vaste du gouvernement fédéral visant à favoriser la sensibilisation à la protection de l'information numérique en général.[1] En fait, la publication du Préavis survient environ trois mois après l'introduction d'une série d'obligations en matière de déclaration prévues par la *Loi sur la protection des renseignements personnels et les documents électroniques* (la « **LPRPDE** »), qui s'appliquent à toutes les organisations du secteur privé dont la sécurité des renseignements personnels dont elles ont la gestion a été atteinte.[2]

Critères de signalement des incidents

Le Préavis prévoit que les IFF doivent signaler au BSIF certains incidents liés à la technologie ou à la cybersécurité. Dans le cadre du Préavis, un incident lié à la technologie ou à la cybersécurité s'entend d'un incident 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 ».

Les incidents dont le « niveau de gravité » est jugé « élevé ou critique » doivent être signalés au BSIF.

Bien que les IFF devraient définir les critères permettant d'établir l'importance relative d'un incident dans leur cadre de gestion des incidents et de la cybersécurité (lequel devrait, ultimement, être évalué par l'IFF en fonction des exigences prévues par les Conseils sur la cybersécurité), le Préavis contient une liste non exhaustive des caractéristiques qu'un incident à signaler peut présenter :

- répercussions opérationnelles importantes sur les systèmes d'information ou les données critiques;
- répercussions importantes sur les données opérationnelles ou sur les données des clients de l'IFF, y compris sur les plans de la confidentialité, de l'intégrité ou de la disponibilité de ces données;
- répercussions opérationnelles importantes pour les utilisateurs à l'interne, lesquelles entraînent à leur tour des conséquences importantes pour les clients ou sur les activités opérationnelles;
- niveaux importants de perturbation des systèmes et des services;
- perturbations prolongées des systèmes et activités essentiels;
- nombre important ou croissant de clients externes touchés;
- répercussions négatives imminentes sur la réputation (p. ex., divulgation publique/médiatique);
- répercussions importantes sur les échéances/obligations cruciales rattachées aux systèmes de règlement ou de paiement des marchés financiers (p. ex., infrastructure des marchés financiers);
- répercussions importantes sur un tiers essentiel pour l'IFF;
- conséquences importantes pour les autres IFF ou pour le système financier canadien;
- l'incident a été signalé au Commissariat à la protection de la vie privée du Canada ou aux organismes de réglementation canadiens/étrangers.

Exigences de signalement initial

Si une IFF considère qu'un incident présente les caractéristiques énoncées dans le Préavis ou des caractéristiques semblables à celles-ci, elle doit le signaler au BSIF le plus rapidement possible, mais au plus tard 72 heures après avoir déterminé que l'incident devait être signalé. En plus d'informer son chargé de surveillance, l'IFF doit envoyer un courriel de notification à la Division du risque lié à la technologie du BSIF (TRD@osfi-bsif.gc.ca).

Le Préavis précise les éléments que les IFF devraient signaler dans leur rapport d'incident. Par exemple, la description de l'incident devrait indiquer les répercussions connues, si l'incident est survenu à l'interne ou à l'externe, les causes connues ou soupçonnées, et la stratégie d'atténuation. Le BSIF s'attend à ce que les IFF informent quotidiennement le chargé de surveillance de l'état de la situation jusqu'à ce que l'incident soit maîtrisé, et qu'elles fournissent un rapport post-incident faisant état des leçons apprises.

Application

Bien que le Préavis n'ait pas en soi force de loi, le BSIF a certains pouvoirs d'application qui sont prévus par la loi. Par exemple, la *Loi sur les sociétés d'assurances* confère au BSIF de vastes pouvoirs qui lui permettent d'enjoindre aux assureurs de s'abstenir d'adopter une attitude contraire aux bonnes pratiques du commerce ou d'y mettre un terme, ou de prendre les mesures qui, selon lui, s'imposent pour remédier à la situation, selon le cas.[3] Ces décisions sont mises à exécution au moyen d'une ordonnance d'un tribunal[4]. *La Loi sur les banques*[5] renferme également des dispositions semblables. Du point de vue pratique, les IFF devraient considérer que les exigences de signalement contenues dans le Préavis constituent des obligations de leur part et intégrer sans délai les dispositions et les principes pertinents dans leurs cadres d'intervention en cas d'incident respectifs.

Comparaison avec les exigences prévues par la LPRPDE

Depuis le 1er novembre 2018, les organisations assujetties à la LPRPDE doivent déclarer au Commissaire à la protection de la vie privée du Canada ainsi qu'aux personnes touchées toute « atteinte aux mesures de sécurité » qui a trait à des renseignements personnels dont l'organisation a la gestion s'il est raisonnable de croire que l'atteinte présente un « risque réel de préjudice grave » pour ces personnes.

Les exigences de signalement énoncées dans le Préavis diffèrent à quelques égards importants des obligations de déclaration prévues par la LPRPDE. Par exemple, les lignes directrices en matière de signalement contenues dans le Préavis ont un champ d'application plus large que les obligations de déclaration prévues par la LPRPDE du fait qu'elles s'appliquent, peu importe si l'incident concerne ou non des renseignements personnels. Les incidents à signaler en vertu du Préavis doivent présenter un « niveau de gravité élevé ou critique », alors que, en vertu de la LPRPDE, ils doivent présenter un « risque réel de préjudice grave ». Le Préavis prévoit que l'incident doit être signalé dans un délai maximal de 72 heures, alors que la LPRPDE ne fournit aucun détail et mentionne seulement que la déclaration doit être faite « le plus tôt possible » après la découverte de l'atteinte. Enfin, le Préavis mentionne qu'un incident à signaler s'entend d'un incident qui pourrait avoir des conséquences importantes sur les activités habituelles d'une IFF, alors que la LPRPDE ne renferme aucune disposition semblable concernant la portée ou l'importance d'une atteinte à déclarer en vertu de cette loi.

Ententes d'impartition

En attendant la date de prise d'effet du Préavis, les IFF devraient examiner les contrats qu'elles ont conclus avec des fournisseurs de services tiers afin de s'assurer que ces parties sont tenues d'aider l'IFF à remplir ses obligations en vertu du Préavis. De plus, et compte tenu de l'intérêt que le BSIF porte aux activités d'impartition des IFF (étant donné que, par exemple, les fournisseurs de services tiers pourraient avoir des

pratiques de cybersécurité moins rigoureuses et moins de ressources pour gérer une atteinte), les IFF devraient profiter de l'occasion pour évaluer l'ensemble de leur risques liés à l'impartition[6] et si elles devraient prévoir dans les contrats qu'elles concluent avec leurs fournisseurs que ceux-ci doivent souscrire de la cyberassurance ou prendre d'autres mesures de protection.

Dans le contexte actuel où le gouvernement du Canada examine les avantages et les inconvénients potentiels d'un système bancaire ouvert (c'est-à-dire un cadre dans lequel les consommateurs et les entreprises pourraient autoriser des tiers fournisseurs de services financiers à avoir accès à leurs données sur les opérations financières au moyen de canaux sécurisés en ligne)[7] et où des modifications apportées à certaines lois régissant les activités liées à la technologie des IFF sont entrées en vigueur récemment ou sont sur le point de l'être,[8] il n'est pas surprenant que la cybersécurité et la protection des données soient au centre des préoccupations du BSIF.

par Darcy Ammerman, Grace Shaw et John Alsbergas (étudiant en droit)

[1] Voir, par exemple, la publication de 2019 de Sécurité publique Canada, *Stratégie nationale de cybersécurité : Vision du Canada pour la sécurité et la prospérité dans l'ère numérique*.*[ps2id id='1' target='/]*
[2] La *Loi sur la protection des renseignements personnels et les document électroniques*, L.C. 2000, c. 5, art. 10.1, 10.2 et 10.3.[ps2id id='2' target='/]
[3] *Loi sur les sociétés d'assurances*, L.C. 1991, c. 47, art. 676.[ps2id id='3' target='/]
[4] *Ibid*, art. 678[ps2id id='4' target='/]
[5] *Loi sur les banques*, L.C. 1991, c. 47, art. 615, 616, 645, 646, 960 et 961.[ps2id id='5' target='/]
[6] Voir la ligne directrice du BSIF intitulée *Impartition d'activités, de fonctions et de méthodes commerciales,* en date du mois de mars 2009, qui pourrait être utile à cet égard.[ps2id id='6' target='/]
[7]Ministère des Finances du Canada, *Document de consultation : Examen des mérites d'un système bancaire ouvert*, janvier 2019.[ps2id id='7' target='/]
[8] Voir la *Loi no 1 d'exécution du budget de 2018*, L.C. 2018 c. 12, qui a reçu la Sanction royale le 21 juin 2018.[ps2id id='8' target='/]

Mise en garde


mcmillan