OSLER

Le BSIF énonce ses attentes en matière de signalement des incidents liés à la technologie et à la cybersécurité

19 MARS 2019 6 MIN DE LECTURE

Expertises Connexes

- Cybersécurité et intervention en cas d'incident lié à la sécurité
- Opérations commerciales technologiques
- Services bancaires et financiers
- Services financiers
- Technologie

Le Bureau du surintendant des institutions financières (BSIF) du Canada a récemment publié un *préavis de signalement des incidents liés à la technologie et à la cybersécurité,* qui entre en vigueur le 31 mars 2019 (le préavis).[1]

Le préavis établit les attentes du BSIF à l'égard des institutions financières fédérales (IFF) concernant le signalement d'incidents liés à la technologie et à la cybersécurité qui touchent les activités des IFF. Le préavis définit un incident lié à la technologie ou à la cybersécurité comme 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 (l'incident). Le préavis précise en outre que les IFF doivent signaler l'incident au BSIF (en avisant leur chargé de surveillance ainsi qu'en envoyant un courriel à TRD@osfi-bsif.gc.ca), *par écrit, le plus rapidement possible, et au plus tard 72 heures après avoir déterminé qu'un incident répondait aux caractéristiques énoncées relativement aux incidents.* Le préavis précise ces caractéristiques :

- 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;
- Un incident concernant une IFF a été signalé au Commissariat à la protection de la vie privée du Canada ou aux organismes de réglementation canadiens/étrangers.

De plus, le préavis prévoit que les IFF définissent l'importance relative des incidents dans leur cadre de gestion des incidents et qu'elles signalent au BSIF les incidents dont elles estiment

le niveau de gravité élevé ou critique. Une liste des éléments à inclure au moment du signalement initial est fournie, et le préavis indique que le BSIF devrait recevoir des mises à jour périodiques (y compris au sujet des mesures et des plans de redressement à court et à long terme). Le BSIF peut modifier la méthode employée pour les mises à jour subséquentes ainsi que leur fréquence.

Les clients doivent tenir compte des considérations suivantes en évaluant l'incidence de ce préavis :

- Il pourrait être utile de clarifier la formulation du préavis, mais les caractéristiques énoncées semblent être des symptômes ou des exemples d'un événement qui a ou pourrait avoir des répercussions importantes sur les activités habituelles d'une IFF. Si l'événement satisfait déjà à la définition d'un incident, il est fort probable que l'une des caractéristiques énoncées soit aussi présente.
- Les politiques et les protocoles internes devraient être revus pour assurer une harmonisation entre les niveaux de gravité des incidents des IFF et les attentes du BSIF, notamment dans le cadre de ces nouvelles obligations de signalement.
- Les caractéristiques d'un incident à signaler sont assez vagues et générales – par exemple, l'obligation de signalement va jusqu'à découler de « niveaux importants de perturbation des systèmes et des services ». Une telle caractéristique peut aller bien au-delà de ce qu'entend la terminologie type des protocoles internes ou des fournisseurs de service, qui peut se limiter parfois aux incidents liés à la protection des renseignements personnels ou à d'autres incidents liés à la sécurité.
- L'IFF devrait considérer les éléments suivants dans ses ententes actuelles et futures avec des fournisseurs de service : i) l'obligation du fournisseur de service de signaler les incidents à l'IFF; ii) l'obligation du fournisseur de service de fournir suffisamment de détails à l'IFF pour permettre à celle-ci de satisfaire aux exigences de signalement initial et de mises à jour subséquentes de la situation énoncées dans le préavis; et iii) le droit pour l'IFF de partager les renseignements liés à un incident et son signalement avec le BSIF ainsi qu'avec toute tierce partie éventuelle dont l'IFF a retenu les services pour l'aider à gérer l'incident ou à mener une enquête.
- En outre, bien que la plupart des ententes conformes au seuil prescrit par la ligne directrice B-10 du BSIF sur l'impartition entrent probablement dans le champ d'application d'un tel examen, il faut noter que la portée du préavis ne se limite pas aux ententes importantes en matière d'impartition et qu'elle inclut tous les incidents liés aux fournisseurs de service dans le cadre desquels les répercussions sur l'IFF satisfont aux critères énoncés dans le préavis.

L'Annexe au préavis guide les IFF en donnant des exemples d'incidents liés à la technologie ou à la cybersécurité qui doivent être signalés au BSIF, conformément au préavis. Cependant, si vous avez des doutes concernant le signalement d'un tel événement, n'hésitez pas à communiquer avec le groupe Technologie d'Osler.

[1] Le BSIF s'attend à ce que les IFF continuent de signaler les incidents majeurs selon les directives préalablement communiquées par leurs chargés de surveillance jusqu'à ce que le préavis entre en vigueur, le 31 mars 2019. À partir de cette date, le préavis l'emportera sur toute directive antérieure concernant le signalement d'incidents liés à la technologie et à la cybersécurité.