Préavis

Catégorie : Surveillance

Objet : Signalement des incidents liés à la technologie et à la cybersécurité

Date d'entrée en vigueur : 13 août 2021

But

Le préavis intitulé *Signalement des incidents liés à la technologie et à la cybersécurité* soutient l'adoption d'une approche coordonnée et intégrée pour la prise de connaissance par le BSIF des incidents liés à la technologie et à la cybersécurité qui touchent les activités des institutions financières fédérales (IFF) et sa réponse à ces incidents. Il remplace le préavis *Signalement des incidents liés à la technologie et à la cybersécurité* actuel, publié en janvier 2019 et est entrée en vigueur en mars 2019.

En tant que membres d'un secteur essentiel pour l'économie canadienne, les IFF doivent réagir promptement et efficacement aux incidents liés à la technologie et à la cybersécurité. Si de tels incidents se produisent dans le cadre de leurs activités, elles doivent les signaler rapidement au BSIF, ce qui doit être précisé dans leurs politiques et procédures.

Le signalement des incidents peut aider à repérer les points que les IFF ou l'ensemble du secteur pourraient améliorer pour prévenir de tels incidents de façon proactive ou renforcer leur résilience dans les cas où un incident s'est produit.

Portée et définition

Le présent préavis s'applique à toutes les IFF et décrit les exigences du BSIF en matière de signalement des incidents. Il ne comprend pas de conseils sur les attentes du BSIF à l'égard d'un cadre de gestion des incidents.

Dans le présent préavis, un incident lié à la technologie ou à la cybersécurité s'entend d'un incident qui a ou pourrait avoir des conséquences sur les activités 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.

Critères de signalement

Les IFF doivent définir les niveaux de priorité et de gravité des incidents dans leur cadre de gestion des incidents. En cas de doute quant à savoir si elles doivent signaler un incident, les IFF doivent consulter leur chargé de surveillance.

Un incident à signaler peut présenter n'importe laquelle des caractéristiques suivantes :

- Conséquences importantes pour les autres IFF ou pour le système financier canadien;
- Répercussions sur les systèmes des IFF touchant les règlements, la confirmation ou les paiements sur les marchés financiers (p. ex. : infrastructure des marchés financiers), ou sur les services de paiement;
- Répercussions sur les activités, les infrastructures, les données ou les systèmes des IFF, y compris sur la confidentialité, l'intégrité ou la disponibilité des données des clients;
- Perturbations des systèmes ou des activités, y compris des pannes des services publics ou des centres de données ou la perte ou la dégradation de la connectivité;
- Répercussions opérationnelles sur les systèmes, les infrastructures ou les données essentiels;
- Activation des équipes ou des plans de reprise après sinistre ou déclaration de sinistre par un fournisseur externe ayant des répercussions sur l'IFF;
- Répercussions opérationnelles pour les utilisateurs internes, lesquelles entraînent à leur tour des conséquences pour les clients externes ou les activités opérationnelles;
- Nombre croissant de clients externes touchés et répercussions négatives imminentes sur la réputation (p. ex., divulgation publique/médiatique);
- Répercussions sur un tiers ayant des conséquences pour l'IFF;
- Activation de l'équipe ou des protocoles de gestion des incidents liés à la technologie et à la cybersécurité d'une IFF;
- Signalement d'un incident au conseil d'administration ou à la haute direction;
- Signalement d'un incident concernant une IFF à l'une des entités suivantes :
    - Commissariat à la protection de la vie privée;
    - autre organisme fédéral (p. ex. Centre canadien pour la cybersécurité);
    - autres organismes de surveillance ou de réglementation canadiens ou étrangers;
    - forces de l'ordre;
- Incident ayant requis l'intervention d'un conseiller interne ou externe;
- Incident survenu à une IFF pour lequel une réclamation d'assurance contre le cyberrisque a été soumise;
- Incident dont l'IFF estime que le niveau de gravité est élevé ou critique (niveau de priorité/gravité 1 ou 2 selon l'évaluation interne de l'IFF);
- Incident lié à la technologie ou à la cybersécurité qui fait en sorte que les seuils internes de tolérance au risque ou de propension à prendre des risques ne sont pas respectés.

Si un incident ne présente aucune des caractéristiques susmentionnées, ou si l'IFF hésite quant à la marche à suivre, il est conseillé de le signaler au BSIF à titre de précaution.

Exigences de signalement initial

L'IFF doit aviser la Division du risque lié aux technologies et son chargé de surveillance le plus rapidement possible, et **au plus tard dans les 24 heures suivant** l'incident.

Lorsqu'une IFF signale un incident lié à la technologie ou à la cybersécurité au BSIF, elle doit aviser la Division du risque lié aux technologies (TRD@osfi-bsif.gc.ca) et son chargé de surveillance **par écrit** (par voie électronique[1]), comme prévu dans le formulaire de signalement et de résolution d'un incident (voir l'annexe II). Si des renseignements importants ne sont pas disponibles au moment du signalement initial, l'IFF doit indiquer que « l'information n'est pas encore disponible », auquel cas elle doit fournir les meilleures estimations possible et tous les autres renseignements disponibles à ce moment.

Exigences de signalement subséquent

Le BSIF s'attend à ce que les IFF fassent périodiquement le point (p. ex., tous les jours) à mesure que de nouveaux renseignements deviennent disponibles, et ce, jusqu'à ce que tous les renseignements importants au sujet de l'incident aient été fournis.

Selon la gravité et les conséquences de l'incident et la vitesse à laquelle il se matérialise, le BSIF peut demander à une IFF de modifier la méthode employée pour faire les mises à jour subséquentes ainsi que leur fréquence.

Jusqu'à ce que l'incident soit maîtrisé ou résolu, le BSIF s'attend à ce que les IFF fassent le point sur la situation, y compris au sujet des mesures et des plans de redressement à court et à long terme.

Une fois l'incident maîtrisé, les activités reprises et le dossier clos, l'IFF doit rendre compte au BSIF de son examen postérieur à l'incident et des leçons apprises.

Défaut de signaler

Si l'IFF omet de signaler un incident comme indiqué ci-dessus, elle s'expose à une surveillance accrue, notamment des activités de suivi renforcées, à son inscription à la liste de surveillance ou à son classement à un stade d'intervention.

[1] S'il est impossible de procéder par voie électronique, l'IFF peut aviser le BSIF par téléphone puis sur papier.

Annexe I – Exemples d'incidents à signaler

Le tableau qui suit donne des exemples d'incidents à signaler, mais ne doit pas être considéré comme une liste exhaustive.

Scénario	Description du scénario	Conséquences
Cyberattaque	Attaque robotisée de prise de contrôle des comptes ciblant les services en ligne à l'aide de nouvelles techniques; les moyens de défense actuels n'empêchent pas la compromission des comptes clients	Tentatives nombreuses en peu de temps Les contrôles en place ne bloquent pas l'attaque Les clients sont privés d'accès Indication que les comptes ou les renseignements des clients ont été compromis
Disponibilité et rétablissement des services	Défaillance technologique au centre de données	Un service en ligne essentiel est en panne et les mesures de contournement ont échoué Perturbation prolongée des systèmes et des activités critiques
Compromission liée à un tiers	Les données ou systèmes utilisés par un tiers important ont été compromis; l'IFF est avisée que le tiers fait enquête	Il s'agit d'un tiers désigné comme étant important pour l'IFF Des répercussions sur les données de l'IFF sont possibles
Menace d'extorsion	L'IFF a reçu un message d'extorsion qui laisse entendre qu'une cyberattaque sera commise (p. ex., attaque par DDoS pour obtenir des Bitcoins)	La menace est crédible Probabilité de perturbation des services critiques en ligne

ANNEXE II – Formulaire de signalement et de résolution d'un incident – BSIF

Les IFF doivent utiliser ce formulaire pour signaler un incident à la Division du risque lié aux technologies (TRD@osfi-bsif.gc.ca) et à leur chargé de surveillance.

Signalement d'un incident lié à la technologie ou à la cybersécurité		
1. Renseignements sur l'incident et coordonnées	**Nom ou identifiant de l'incident :**	
	Date et heure de découverte/détection de l'incident :	**Date et heure de survenance de l'incident :**
	Nom de votre institution :	
	Nom de la principale personne-ressource	Poste de la principale personne-ressource
	Adresse courriel de la principale personne-ressource	Numéro de téléphone de la principale personne-ressource
	Nom du responsable de la gestion de l'incident	Poste du responsable de la gestion de l'incident
2. Site/emplacement et secteurs d'activité touchés	Nom des secteurs d'activité touchés	
	Technologies touchées	
	Site ou emplacement touché	
3. Description du risque et de l'incident	Indiquer le type d'incident (p. ex. rançongiciel, hameçonnage, DDoS, etc.). Choisir une option dans la liste déroulante.	Type de renseignements : IPI/confidentiels, renseignements sur le compte, etc. Choisir une option dans la liste déroulante.
	Fournir des précisions concernant les outils, techniques et processus impliqués dans l'incident.	Fournir les indicateurs de compromission.
4. Niveau ou priorité de l'incident	Sélectionner un niveau de gravité ou de priorité dans la liste déroulante.	
5. État actuel	**Fournir des précisions concernant l'état actuel, les mesures achevées et en attente et les délais prévus pour remédier à l'incident. Inclure la cause première ou les causes connues de l'incident.**	
	Notifications internes et externes	
	Les cadres supérieurs ont-ils été prévenus?	Date et heure où les cadres supérieurs ont été prévenus (le cas échéant).
	D'autres organismes de réglementation ou de surveillance ont-ils été prévenus?	Date et heure où les organismes de réglementation ou de surveillance ont été prévenus (le cas échéant).
	Nom des autres organismes de réglementation ou de surveillance ayant été prévenus.	
	Les forces de l'ordre ont-elles été prévenues?	Nom des forces de l'ordre ayant été prévenues.
	Des fournisseurs de services d'assurance contre le cyberrisque ont-ils été prévenus?	Nom des fournisseurs de services d'assurance contre le cyberrisque ayant été prévenus et date de notification.
	Une réclamation d'assurance (contre le cyberrisque ou autre) a-t-elle été présentée?	A-t-on retenu les services d'une firme d'enquête externe?
	L'expert en compromission a-t-il été prévenu?	A-t-on fait appel à un conseiller juridique interne ou externe?