Transmis par courriel à : consultation-en-cours@lautorite.qc.ca

Montréal, le 13 février 2025

Me Philippe Lebel
Secrétaire et directeur général du secrétariat et des affaires juridiques
Autorité des marchés financiers
Place de la Cité
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1

Objet : Consultation – Nouveau formulaire de l'Autorité des marchés financiers pour le signalement des incidents de sécurité de l'information

Monsieur,

L'Association canadienne des compagnies d'assurances de personnes (l'ACCAP) apprécie l'occasion qui lui est donnée de présenter ses commentaires dans le cadre de la consultation sur le formulaire de signalement des incidents de sécurité de l'information relatif au *Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit* publié dans le Bulletin de l'Autorité des marchés financiers (l'Autorité) le 16 janvier 2025.

Nous vous soumettons dans les paragraphes suivants des commentaires généraux visant le formulaire ainsi que des recommandations portant plus précisément sur certaines sections.

COMMENTAIRES GÉNÉRAUX

Advenant un incident de sécurité de l'information au sein d'une institution financière visée par le Règlement, celle-ci sera soumise à diverses déclarations auprès des organismes de réglementation.

Dans un premier temps, le présent formulaire devra être utilisé pour signaler l'incident à l'Autorité, transmettre les avis sur l'évolution de la situation et faire parvenir le rapport final une fois l'incident maîtrisé.

En parallèle, les institutions financières à charte fédérale devront remplir un formulaire distinct de divulgation des incidents de sécurité de l'information à l'attention du Bureau du surintendant des institutions financières (BSIF).

Et finalement, si l'incident concerne un incident de confidentialité, les organisations devront également, sous certaines conditions, en informer la Commission d'accès à l'information du Québec.[1]

Nous reconnaissons la distinction des mandats des différents organismes et juridictions au Canada ainsi que les exigences qui leur sont propres. Or, dans un contexte où l'on vise à optimiser la charge réglementaire et administrative des organisations afin de favoriser leur efficacité et leur agilité, nous invitons l'Autorité en collaboration avec ses homologues fédéral et provinciaux à élaborer un formulaire de déclaration des incidents de sécurité de l'information unique à l'échelle canadienne.

En avril 2023, le Financial Stability Board mentionnait dans son rapport *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report - Financial Stability Board* que « *les autorités financières devraient identifier individuellement ou collectivement des exigences communes en matière de données et, le cas échéant, élaborer ou adopter des formats normalisés pour l'échange d'informations relatives aux incidents. »*[2] *[Traduction]*

Nous sommes convaincus que cette voie permettrait aux organisations d'améliorer l'efficacité de leur politique de déclaration des incidents de sécurité et ultimement favoriserait une meilleure gestion des incidents eux-mêmes.

COMMENTAIRES SPÉCIFIQUES

Type d'incident

La taxonomie proposée dans le formulaire de l'Autorité engendre plusieurs questionnements que nous souhaitons soulever ci-dessous.

a. *Des propositions qui ne sont pas mutuellement exclusives*

La taxonomie des types d'incidents telle que proposée comprend des catégories qui ne s'excluent pas mutuellement. Par exemple, si une organisation reçoit un courriel d'hameçonnage et qu'en cliquant dessus, celui-ci exécute une commande malveillante qui lui permet d'accéder à son système local (accès non autorisé) et éventuellement d'enclencher une commande de rançongiciel, nous nous interrogeons sur le type d'incident qui devrait être sélectionné dans la déclaration.

Nous nous questionnons à savoir si plusieurs catégories pourront être sélectionnées ou s'il sera requis de choisir une seule réponse. Advenant ce cas, la catégorie devant être sélectionnée devrait-elle être déterminée par le type initial d'incident, par le type de commande enclenchée ou encore par l'action finale exécutée?

[1] *Loi sur la protection des renseignements personnels dans le secteur privé,* article 3.5.

[2] **Recommendations to Achieve Greater Convergence in Cyber Incident Reporting**, Financial Stability Board, April 13, 2023, page 1: "*Financial authorities should individually or collectively identify common data requirements, and, where appropriate, develop or adopt standardised formats for the exchange of incident reporting information.*"

b. Définition de type d'incident

Les types d'incidents soumis dans la liste du formulaire présentent différentes options qui, selon nous, s'assimilent plutôt à des causes d'incidents. Par exemple, une « erreur humaine », la « vulnérabilité » d'un système informatique ou le « piratage psychologique » correspondent plutôt à des causes qui pourraient mener à un incident plutôt qu'au type d'incident lui-même.

D'autres juridictions considèrent d'ailleurs ces éléments comme des choix de causes ayant entraîné un incident de sécurité de l'information. Ainsi, afin d'éviter les risques de confusion quant à la terminologie utilisée, il serait important de réviser la liste des incidents proposés.

Nous recommandons de retirer les options « erreur humaine », « vulnérabilité » d'un système informatique et « piratage psychologique » de la liste des types d'incidents possibles et de les intégrer à titre d'exemples dans la section des « Causes de l'incident ».

c. Clarification pour certains types d'incidents

Certains types d'incidents proposés nécessiteraient par ailleurs d'être précisés. C'est le cas notamment de la « Fraude » qui d'un point de vue opérationnel ne correspond pas à un type d'incident de sécurité de l'information, mais se qualifie plutôt comme le résultat d'un tel incident. **Nous recommandons de retirer cette option de la liste des types d'incidents.**

Par ailleurs, nous souhaiterions obtenir des précisions afin de mieux comprendre les attentes de l'Autorité concernant les types d'incidents suivants : « Panne de système » et « Erreur de système ».

<u>Détection et occurrence de l'incident</u>

De manière générale, nous nous interrogeons sur la nécessité d'identifier l'heure de détection ou de l'occurrence d'un incident de sécurité. Il s'agit d'une information très précise qui vient complexifier le processus de déclaration. **Nous recommandons de simplifier la déclaration en se concentrant uniquement sur la date de l'occurrence et de la détection de l'incident.**

D'autre part dans certaines circonstances, il est possible qu'un incident se produise à plusieurs reprises avant que celui-ci ne soit détecté. Il devient alors difficile d'identifier le moment exact de la première occurrence de l'incident.

Nous proposons qu'il soit possible de compléter l'information de la section « Date et heure de l'occurrence de l'incident » sous la forme d'une période de temps ou à tout le moins qu'il soit clarifié que l'occurrence de l'incident déclarée dans le formulaire n'est pas nécessairement la première.

<u>Statut de l'incident</u>

Le formulaire de l'Autorité propose trois statuts permettant de qualifier l'état dans lequel un incident se situe soit « Ouvert », « Maîtrisé » ou « Fermé ». Un délai de 30 jours s'enclenche automatiquement entre le moment où l'incident est identifié comme « Maîtrisé » et l'envoi du rapport post-mortem amenant à la fermeture de l'incident.

Or dans certaines situations, l'incident de sécurité pourrait être qualifié de « maîtrisé », en considérant que les activités ont repris leur cours normal, alors que son analyse est encore en cours et nécessite un délai de plus de 30 jours pour fournir la documentation requise à la fermeture de l'incident.

Par exemple un incident qui concerne la confidentialité de l'information, comme l'accès non autorisé à une boîte de courriels, pourrait faire l'objet d'une enquête pendant un délai dépassant 30 jours alors que les activités n'auront pas été interrompues.

Nous souhaitons porter à l'attention de l'Autorité le fait que certains incidents pourraient nécessiter un délai supérieur à 30 jours pour mener à bien les analyses nécessaires à l'élaboration du rapport post-mortem.

Date et heure de la maîtrise et de la clôture de l'incident

En référence au point précédent, les informations liées à la fermeture d'un incident peuvent poser des difficultés puisque, dans certaines situations, un incident « maîtrisé » pourrait encore faire l'objet d'une enquête au sein de l'organisation. Un délai de 30 jours pourrait alors ne pas suffire pour remplir les exigences requises par règlement afin de fournir un rapport post-mortem.

D'autre part, les précisions requises de l'heure de la maîtrise et de la clôture de l'incident sont des informations qui complexifient la déclaration sans apporter de valeur ajoutée.

Nous recommandons ainsi de retirer l'exigence de fournir l'heure de maîtrise et de clôture de l'incident.

Acteurs

L'identification des acteurs liés à l'incident soulève quelques questions et génère des propositions de modifications que nous souhaitons soumettre ci-dessous.

a. *Noms des intervenants liés à l'incident*

Le formulaire requiert d'identifier « *les intervenants internes ou externes connus qui sont liés à l'incident* » et cite à titre d'exemple un « *employé ou consultant au sein de l'organisation* ».

Nous recommandons que l'identification vise plutôt le rôle de la personne concernée au sein d'une équipe déterminée plutôt que son prénom et son nom. La précision du nom n'apporte pas de valeur ajoutée et la procédure en serait simplifiée.

En ce sens, l'explication fournie par l'Autorité dans le formulaire pourrait être modifiée de la façon suivante :

> *« Veuillez identifier les intervenants internes ou externes connus qui sont liés à l'incident (ex. : ~~employé ou consultant~~ équipe ou service au sein de l'organisation, organisation malveillante reconnue) […] »*

b. Localisation des intervenants liés à l'incident

L'Autorité pourrait-elle préciser le niveau d'information attendu concernant la localisation des intervenants liés à l'incident?

Date et heure des signalements aux parties prenantes prévues au règlement

a. Suggestions de modifications

Afin de faciliter l'application de cette section, nous souhaitons soumettre quelques modifications permettant de clarifier les attentes du régulateur :

- L'ajout suivant vise à clarifier et circonscrire les communications visées par le formulaire :

  « Veuillez préciser la date et l'heure auxquelles vous avez communiqué l'existence de cet incident aux parties prenantes suivantes conformément aux critères de déclaration définis dans votre politique de gestion des incidents : »

- Dans la liste des parties prenantes citées, nous suggérons des modifications permettant d'harmoniser les formulations et de mieux définir les attentes de l'Autorité :

  « Dirigeants ou, selon le cas, gestionnaires (haute direction) » : cet ajout permettrait d'harmoniser les formulations avec la ligne précédente du formulaire.

  « Tiers à qui votre organisation a confié l'exercice de toute partie d'une activité, dans la mesure où l'incident affecte l'activité qui lui a été confiée » : cet ajout permettrait de mieux circonscrire les tiers visés tout en se coordonnant avec le texte du Règlement.

- Nous suggérons de retirer la précision de l'heure de signalement pour les parties prenantes prévues par Règlement. L'information ajoute aux organisations un niveau de complexité qui ne semble pas apporter de valeur supplémentaire.

b. Demande de clarification

Dans le cas d'un incident de confidentialité, les signalements auprès de la Commission d'accès à l'information (CAI) sont réalisés une fois que l'organisation a suffisamment d'information en main et que l'impact sur les clients a été établi. Il serait donc possible que certains incidents de sécurité de l'information impliquant un enjeu de confidentialité soient déclarés à l'Autorité avant de l'être auprès de la CAI.

De quelle façon l'Autorité s'attend-elle à ce que les organisations fournissent l'information concernant le moment du signalement à la CAI dans le cas où celui-ci serait réalisé après la déclaration auprès de l'Autorité?

Clientèles affectées et volumétrie

L'Autorité peut-elle préciser ce qui est entendu dans son texte explicatif par la formulation *« transactions mises en jeu dans l'incident »* ainsi que par la notion de *« répartition géographique »*?

Réactions du public ou d'autres parties prenantes

Telle que formulée dans le formulaire, cette section a une portée très large et serait complexe à remplir. Nous suggérons les modifications suivantes pour permettre de mieux circonscrire la demande.

- Limiter les attentes de cette partie du formulaire aux réactions du public et retirer dans le titre la mention concernant *« les autres parties prenantes ».*

- Par ailleurs, les incidents déclarés ne généreront pas tous une réaction du public. Nous suggérons donc d'apporter la modification suivante au texte descriptif du formulaire :

« Nature et origine des réactions ~~des diverses parties prenantes externes~~ connues à ce jour du public, le cas échéant. »

Communications externes émises à ce jour

Cette section semble redondante avec celle qui, précédemment dans le formulaire, demande les informations de date et heure des signalements aux parties prenantes prévues par le Règlement.

La portée de cette section semble également très large. Nous recommandons qu'elle soit mieux délimitée pour cibler les communications externes générales émises par l'organisation et, par le fait même, exclure les communications spécifiques adressées aux fournisseurs et clients concernés par l'incident.

Risques résiduels

À des fins de clarification dans l'utilisation de la terminologie de « risques résiduels », nous recommandons de modifier l'intitulé de cette section pour « Potentiel de récurrence de l'incident » qui cible plus clairement l'objectif de cette section du formulaire.

CONCLUSION

Nous vous remercions de nous avoir donné l'occasion de soumettre nos commentaires concernant le formulaire de signalement des incidents de sécurité de l'information. Nous restons disponibles pour en discuter plus amplement. Pour ce faire, veuillez contacter : Typhaine Letertre, Directrice, Politiques publiques, à l'adresse suivante : tletertre@clhia.ca.