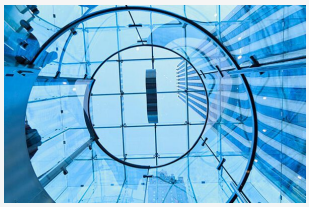
OSLER

Nouvelles règles de la SEC exigeant la publication d'information sur la cybersécurité et répercussions pour les émetteurs canadiens



21 AOÛT 2023 20 MIN DE LECTURE

Expertises Connexes

- Gestion de risques et réponse aux crises
- Gouvernance d'entreprise
- Respect de la vie privée et gestion de l'information

Auteur: Jason Comerford

Le 26 juillet 2023, la Securities and Exchange Commission (SEC) des États-Unis a adopté des règles définitives [PDF; en anglais seulement] exigeant des sociétés ouvertes qu'elles publient de l'information sur les incidents, la gestion des risques et la gouvernance liés à la cybersécurité. Les nouvelles règles s'appliquent à la plupart des émetteurs nationaux américains, ainsi qu'aux émetteurs privés étrangers devant produire le formulaire 20-F (EPE), mais ne s'appliquent pas aux émetteurs canadiens devant produire le formulaire 40-F dans le cadre du régime d'information multinational États-Unis–Canada (RIM).

Les émetteurs nationaux américains doivent déclarer les incidents importants liés à la cybersécurité sur le formulaire 8-K dans les quatre jours ouvrables suivant la détermination de l'importance de l'incident, et doivent fournir chaque année une description de leurs pratiques en matière de gestion des risques, de stratégie et de gouvernance liés à la cybersécurité. Les EPE doivent déclarer sans délai sur le formulaire 6-K les incidents importants liés à la cybersécurité qu'elles déclarent ou rendent publics d'une autre manière dans un territoire étranger, aux bourses de valeurs ou aux porteurs de titres, et doivent fournir chaque année dans le formulaire 20-F une description de leurs pratiques en matière de gestion des risques, de stratégie et de gouvernance liés à la cybersécurité.

L'approche adoptée dans les règles exigeant la déclaration rapide des incidents importants liés à la cybersécurité influera probablement sur les pratiques d'information occasionnelle des émetteurs canadiens au fil du temps et leur application de l'Avis multilatéral 51-347 du personnel des ACVM – *Information sur les risques et les incidents liés à la cybersécurité* [PDF], qui a été publié par les Autorités canadiennes en valeurs mobilières (ACVM) en janvier 2017.

Vue d'ensemble

L'adoption par la SEC des nouvelles obligations d'information a été motivée par sa perception que, malgré l'augmentation substantielle des incidents liés à la cybersécurité au fil du temps, les sociétés ont eu tendance à ne pas les signaler de manière satisfaisante, et que, en ce qui concerne la communication d'information sur la cybersécurité, les approches étaient incohérentes. La SEC avait déjà publié des directives sur la communication d'information sur la cybersécurité en 2011 et en 2018 [PDF; en anglais seulement]. Cependant, la SEC a indiqué

que, selon elle, les directives précédentes n'avaient pas suffisamment permis d'améliorer les pratiques en ce qui concerne la communication d'information sur la cybersécurité et qu'il était nécessaire de rendre certaines pratiques obligatoires pour que les investisseurs soient en mesure de localiser, d'interpréter et d'analyser l'information dont ils ont besoin.

Les nouvelles règles s'appliquent à tous les émetteurs nationaux américains et aux EPE, mais ne s'appliquent pas expressément aux émetteurs de titres adossés à des créances et aux émetteurs canadiens qui déposent des rapports annuels sur formulaire 40-F auprès de la SEC dans le cadre du RIM. Même si les émetteurs recourant au RIM ne sont pas soumis à ces règles, les nouvelles obligations d'information occasionnelle applicables aux incidents importants liés à la cybersécurité influeront probablement sur les pratiques d'information occasionnelle des émetteurs recourant au RIM en vertu des lois canadiennes sur les valeurs mobilières.

Dans les règles définitives, la SEC fournit des directives sur la manière dont les émetteurs doivent déterminer l'importance d'un incident important lié à la cybersécurité. Si on considère que les nouvelles règles améliorent la qualité et la rapidité de l'information sur les questions de cybersécurité pour l'application des lois américaines sur les valeurs mobilières, elles influeront probablement sur le mode de détermination de l'importance pour l'application des lois canadiennes sur les valeurs mobilières. L'une des principales différences entre les approches américaine et canadienne est que la SEC exige le dépôt d'un formulaire 8-K dans les quatre jours ouvrables suivant la détermination de l'importance de l'incident lié à la cybersécurité, alors qu'en vertu des lois canadiennes sur les valeurs mobilières et des exigences des bourses de valeurs, un communiqué doit être publié immédiatement après la détermination de l'importance de la brèche de cybersécurité.

Résumé des nouvelles obligations d'information

Document	Informations à fournir
Déclaration des incidents	
Rapports courants sur formulaire 8-K	Les émetteurs nationaux américains doivent déclarer sur le formulaire 8-K tout incident lié à la cybersécurité qu'ils déterminent comme important et décrire les aspects importants i) de sa nature, de sa portée et de sa chronologie et ii) de son incidence ou de l'incidence qu'il est raisonnablement susceptible d'avoir. Le formulaire 8-K doit être déposé dans les quatre jours ouvrables suivant la détermination de l'importance de l'incident, mais le dépôt peut être retardé si le procureur général des États-Unis détermine qu'une déclaration immédiate soulèverait un risque substantiel pour la sécurité nationale ou la sécurité publique. Le délai de quatre jours ouvrables doit être respecté même si certains éléments d'information à fournir n'ont pas été déterminés ou n'étaient pas disponibles au moment du dépôt du formulaire 8-K. Un formulaire 8-K modifié doit être déposé une fois que ces éléments d'information ont été déterminés ou sont devenus disponibles.
Rapports courants sur formulaire 6-K	Les EPE doivent fournir sur le formulaire 6-K l'information sur les incidents importants liés à la cybersécurité qu'elles déclarent ou rendent publics d'une autre manière dans un territoire étranger, aux bourses de valeurs ou aux porteurs de titres.
Informations à fournir dans le rapport annuel	
Rapport annuel sur formulaire 10-K	

Information sur les risques liés à la cybersécurité	Les émetteurs nationaux américains doivent décrire les processus qu'ils mettent en œuvre pour évaluer, repérer et gérer les risques importants liés aux cybermenaces, et indiquer si ces risques ont eu ou sont raisonnablement susceptibles d'avoir une incidence importante sur leur stratégie commerciale, leurs résultats d'exploitation ou leur situation financière.
Gouvernance liée à la cybersécurité	Les émetteurs nationaux américains doivent décrire i) la manière dont leur conseil d'administration surveille les risques liés aux cybermenaces et ii) le rôle de la direction dans l'évaluation et la gestion des risques importants liés aux cybermenaces.
Rapport annuel sur formulaire 20-F	Les EPE doivent décrire i) la manière dont leur conseil d'administration surveille les risques liés aux cybermenaces et ii) le rôle de la direction dans l'évaluation et la gestion des risques importants liés aux cybermenaces.

Déclaration des incidents importants liés à la cybersécurité

Les nouvelles règles exigent que les incidents importants liés à la cybersécurité soient déclarés sur le formulaire 8-K ou le formulaire 6-K, selon le cas. Un « incident lié à la cybersécurité » (*cybersecurity incident*) s'entend d'une [TRADUCTION LIBRE] « activité non autorisée ou une série d'activités non autorisées connexes, survenant sur ou via les systèmes d'information de l'émetteur inscrit, qui compromet la confidentialité, l'intégrité ou la disponibilité des systèmes d'information de l'émetteur inscrit ou de toute information qui y réside ». Dans le communiqué final, la SEC a précisé que toute activité « accidentelle » devait être considérée comme une « activité non autorisée ».

La SEC a également indiqué qu'il pouvait y avoir des cas, même s'ils étaient rares, où la menace causée par un incident lié à la cybersécurité pouvait avoir une incidence importante sur la société, même si l'incident n'a pas encore causé de dommages réels. Enfin, la SEC a précisé que les systèmes d'information de l'émetteur comprenaient les systèmes de tiers utilisés par l'émetteur, tels que les services de stockage et de partage de fichiers.

Moment de la déclaration

Lorsqu'il prend connaissance d'un incident lié à la cybersécurité, l'émetteur doit évaluer si l'incident est important en se fondant sur la manière dont un investisseur raisonnable considérerait l'incidence de l'incident sur l'émetteur. Les émetteurs devant produire un formulaire 8-K doivent déterminer l'importance « sans retard indu » (*without unreasonable delay*); toutefois, dans le communiqué final, la SEC a indiqué que l'importance ne devait pas être déterminée le jour même de la découverte de l'incident. S'il est déterminé que l'incident lié à la cybersécurité est important, sa déclaration sur le formulaire 8-K doit avoir lieu dans les quatre jours ouvrables suivant la détermination. Toutefois, si le procureur général des États-Unis détermine que la déclaration de l'incident soulèverait un risque substantiel pour la sécurité nationale ou la sécurité publique, l'émetteur peut retarder le dépôt du formulaire 8-K pendant la période déterminée par le procureur général des États-Unis, d'au plus 30 jours, période qui peut être prolongée de 60 jours dans des circonstances extraordinaires où le procureur général des États-Unis détermine que la déclaration continue de soulever un risque substantiel pour la sécurité nationale.

La SEC précise dans le communiqué final que l'importance doit être déterminée suivant le critère d'importance prévu par les lois sur les valeurs mobilières en général, soit la question de savoir s'il existe une forte probabilité qu'un actionnaire raisonnable considère l'incident comme important pour la prise d'une décision en matière de placement ou si l'incident modifie de manière importante l'ensemble de l'information disponible. La SEC note que la détermination de l'importance tient de l'analyse des faits et qu'un incident lié à la cybersécurité qui touche plusieurs émetteurs pourrait devoir faire l'objet d'une déclaration de la part de certains d'entre eux seulement, ou pourrait ne pas devoir être déclaré au même

moment par la totalité d'entre eux. La SEC a noté qu'une série de cyberattaques liées, chacune constituant en soi un incident sans importance, pourrait, lorsqu'on les considère dans leur ensemble, devenir importante.

Informations à fournir

La nouvelle rubrique 1.05 du formulaire 8-K exigera des émetteurs qu'ils décrivent les aspects importants de la nature, de la portée et de la chronologie de l'incident lié à la cybersécurité, ainsi que son incidence importante ou l'incidence importante qu'il est raisonnablement susceptible d'avoir sur l'émetteur, y compris sa situation financière et ses résultats d'exploitation. La SEC a noté que l'inclusion de la référence à la situation financière et aux résultats d'exploitation n'est pas exclusive et que les émetteurs doivent prendre en compte des facteurs qualitatifs en plus des facteurs quantitatifs, tels que les relations avec les clients et les fournisseurs, la réputation, la compétitivité ou le risque de litige. Pour répondre aux préoccupations selon lesquelles les émetteurs ne devraient pas être tenus de fournir des informations qui pourraient être utiles aux auteurs des cybermenaces, la SEC a ajouté à la rubrique 1.05 une instruction portant qu'il n'est pas nécessaire de présenter des informations précises ou techniques sur l'intervention que l'émetteur entend mener relativement à l'incident ou sur ses systèmes de cybersécurité, les réseaux et dispositifs connexes ou les vulnérabilités potentielles des systèmes de manière si détaillée qu'elles entraveraient l'intervention de l'émetteur ou les mesures correctives qu'il entend prendre.

Si l'une des informations à fournir n'est pas disponible ou est indéterminée au moment du dépôt du formulaire 8-K, l'émetteur doit déposer une mise à jour sur un formulaire 8-K modifié dans les quatre jours ouvrables suivant la date à laquelle l'information devient disponible.

Bien que les émetteurs ne soient pas tenus d'indiquer l'état des mesures correctives prises relativement à l'incident, si les travaux sont en cours ou si des données ont été compromises, ou encore de fournir des informations précises sur leur intervention, le communiqué final note que les émetteurs peuvent choisir de leur plein gré de fournir ces informations dans leur déclaration.

Lorsque l'incident lié à la cybersécurité survient dans un système tiers utilisé par l'émetteur, les règles exigent de l'émetteur qu'il ne fournisse que les informations auxquelles il a accès, et ne l'obligent pas de mener des enquêtes supplémentaires.

Les informations sur les incidents importants liés à la cybersécurité bénéficient d'un régime limité de protection de la responsabilité en vertu du paragraphe 10(b) de la loi américaine intitulée *Securities Exchange Act of 1934* et de la *Rule 10b-5* prise en application de celle-ci, et l'émetteur qui dépose sa déclaration hors du délai prévu à la rubrique 1.05 du formulaire 8-K ne perdra pas son droit d'utiliser la déclaration d'enregistrement simplifiée sur formulaire S-3.

Répercussions pour les émetteurs canadiens

De façon générale, l'évaluation de l'importance aux fins de la déclaration sur formulaire 8-K correspond à celle qu'un émetteur canadien doit faire pour déterminer s'il doit déposer une déclaration de changement important en vertu des lois canadiennes sur les valeurs mobilières et des indications fournies dans l'Avis multilatéral 51-347 du personnel des ACVM, et le communiqué de la SEC peut servir de ressource de référence supplémentaire pour cette évaluation. Toutefois, en vertu des lois canadiennes sur les valeurs mobilières, un émetteur doit publier et déposer un communiqué sans délai après avoir déterminé que l'incident lié à la cybersécurité est important, et il n'y a pas de régime de protection prévu par les lois

canadiennes sur les valeurs mobilières relativement à l'information fournie.

Informations à fournir chaque année sur la gestion des risques, la stratégie et la gouvernance liés à la cybersécurité

Les nouvelles règles exigent également que les émetteurs publient chaque année dans le formulaire 10-K ou le formulaire 20-F, selon le cas, de l'information sur leur gestion des risques, leur stratégie et leur gouvernance en matière de cybersécurité.

En ce qui concerne la gestion des risques et la stratégie, les émetteurs doivent fournir de l'information décrivant les éléments suivants :

1. les processus qu'ils mettent en œuvre pour évaluer, repérer et gérer les risques importants liés aux cybermenaces
2. les risques liés aux cybermenaces qui ont eu ou sont raisonnablement susceptibles d'avoir une incidence importante sur leur stratégie commerciale, leurs résultats d'exploitation ou leur situation financière

Les émetteurs doivent décrire leurs processus de manière suffisamment détaillée pour permettre à un investisseur raisonnable de les comprendre, tout en restant dans les limites de l'information qui constitue de l'information importante pour les investisseurs. Ils devront indiquer si et comment leurs processus de cybersécurité ont été intégrés dans leur système ou processus global de gestion des risques et s'ils disposent de processus de surveillance et de repérage des risques importants liés aux cybermenaces associées au recours à tout fournisseur de services tiers.

En outre, pour permettre aux investisseurs de comprendre le niveau de capacité de cybersécurité qui est externalisé, l'émetteur doit également indiquer si des évaluateurs, des consultants, des auditeurs ou d'autres tiers prennent part à ses processus de cybersécurité. Les émetteurs nationaux américains sont tenus de décrire leurs pratiques de surveillance des risques en général dans leurs circulaires de sollicitation de procurations, ce qu'ils peuvent faire en intégrant par renvoi l'information fournie sur la cybersécurité dans leur formulaire 10-K.

En ce qui concerne la gouvernance, les émetteurs doivent fournir de l'information décrivant les éléments suivants :

1. la manière dont le conseil d'administration surveille les risques liés aux cybermenaces, y compris, le cas échéant, le nom de tout comité ou sous-comité du conseil d'administration chargé de la surveillance des risques liés aux cybermenaces et le processus par lequel le conseil d'administration ou le comité en question est informé de ces risques
2. le rôle de la direction dans l'évaluation et la gestion des risques importants liés aux cybermenaces, y compris, le cas échéant :
    1. si des postes de direction ou des comités sont responsables de l'évaluation et de la gestion de ces risques, et lesquels, et l'expertise pertinente de ces personnes ou membres, avec les détails nécessaires pour décrire pleinement la nature de l'expertise (par exemple, une expérience professionnelle antérieure dans le domaine de la cybersécurité, tout diplôme ou certificat pertinent, ou toute connaissance, compétence ou autre expérience dans le domaine de la cybersécurité)

2. les processus par lesquels ces personnes ou comités sont informés de la prévention, de la détection et de l'atténuation des incidents liés à la cybersécurité, de même que des mesures correctives prises à la suite de ces incidents, et en assurent le suivi
3. si ces personnes ou comités communiquent de l'information sur ces risques au conseil d'administration ou à un comité ou sous-comité du conseil d'administration

Contrairement aux règles qu'elle avait proposées, la SEC a choisi de ne pas exiger d'informations précises sur l'expertise des administrateurs en matière de cybersécurité, notant que les processus de cybersécurité sont principalement conçus et administrés au niveau de la direction.

Dates à respecter

Les règles définitives entreront en vigueur le 5 septembre 2023. Les informations à fournir conformément à la rubrique 106 du *Regulation S-K* (c'est-à-dire les informations à fournir par les émetteurs nationaux américains sur la gestion des risques, la stratégie et la gouvernance) et à la rubrique 16K du formulaire 20-F (c'est-à-dire les informations à fournir par les EPE sur les mêmes sujets) doivent l'être dans les rapports annuels pour les exercices devant clore à compter du 15 décembre 2023. Les informations à fournir sur les incidents en vertu de la rubrique 1.05 du formulaire 8-K et du formulaire 6-K devront l'être à partir du 18 décembre 2023, à l'exception des petites sociétés déclarantes, qui disposeront d'un délai supplémentaire de 180 jours pour se conformer aux obligations d'information, soit jusqu'au 15 juin 2024.

Mesures recommandées aux émetteurs canadiens

La grande majorité des émetteurs canadiens dont les titres sont également inscrits à la cote d'une bourse américaine déposeront leurs documents dans le cadre du RIM ou seront autrement admissibles à titre d'EPE et ne seront donc pas assujettis aux obligations d'information concernant la déclaration des incidents liés à la cybersécurité sur le formulaire 8-K dans les quatre jours ouvrables suivant la date à laquelle ils déterminent qu'un incident important lié à la cybersécurité s'est produit. Au lieu de cela, ils seront tenus de déclarer rapidement sur le formulaire 6-K les incidents importants liés à la cybersécurité rendus publics au Canada conformément aux normes d'information canadiennes applicables. Selon les lois canadiennes sur les valeurs mobilières, la nature et la substance de tout incident lié à la cybersécurité doivent être rendues publiques par voie de communiqué dès qu'il est déterminé que l'incident lié à la cybersécurité constitue un changement important (ou un fait important si l'émetteur est soumis à des obligations d'information occasionnelle en vertu des règles d'inscription des bourses de valeurs à la cote desquelles ses titres sont inscrits), et il n'est peut-être pas nécessaire de fournir tous les éléments d'information prescrits par le formulaire 8-K.

Étant donné que les autorités de réglementation et les investisseurs examinent de plus en plus l'information occasionnelle et l'information utile à la prise de décisions concernant les incidents liés à la cybersécurité, il est conseillé à tous les émetteurs canadiens de prendre dès maintenant des mesures pour s'assurer qu'ils respectent les exigences légales applicables et répondent aux attentes des participants aux marchés financiers, telles que les suivantes :

- Revoir leurs contrôles et procédures de communication de l'information existants afin de s'assurer que les incidents liés à la cybersécurité peuvent être communiqués rapidement au personnel approprié, qui pourra déterminer leur importance et prendre des décisions

en matière d'information, comme les membres de la haute direction et le conseiller juridique. Il devrait exister une procédure claire permettant à l'équipe des TI de porter rapidement les incidents liés à la cybersécurité potentiellement importants à l'attention de la haute direction et de l'équipe des affaires juridiques.

- Contrôler étroitement les mécanismes de défense et l'état de préparation des plans d'intervention en cas d'incident lié à la cybersécurité des fournisseurs tiers au moment de leur engagement et sur une base continue par la suite par le biais d'audits périodiques. Les émetteurs devraient mettre en place, avec leurs fournisseurs tiers, des processus de communication directe et rapide qui prévoient l'évaluation et la communication rapides des incidents importants liés à la cybersécurité.
- Veiller à ce que le conseil d'administration et la direction reçoivent une formation complète sur les incidents liés à la cybersécurité et comprennent clairement les obligations d'information potentielles. Envisager également d'ajouter dans les questionnaires destinés aux administrateurs et aux dirigeants des questions relatives à leur expertise en matière de cybersécurité.
- Envisager la création d'un comité de la cybersécurité au sein du conseil d'administration, composé idéalement de membres ayant une expertise en matière de cybersécurité et bénéficiant d'une formation d'appoint périodique, chargé de superviser expressément les questions liées à la cybersécurité.
- Inscrire à l'ordre du jour des réunions du conseil d'administration des comptes rendus réguliers sur la cybersécurité, y compris une revue de l'analyse actuelle, par la direction, des domaines de risque, des domaines nécessitant actualisation et amélioration, de l'état de préparation des systèmes, des incidents liés à la cybersécurité et des mesures correctives.
- Mettre à jour de façon active les programmes de cybersécurité, mettre en œuvre des plans d'intervention en cas d'incident, organiser des exercices de simulation d'intervention en cas d'incident, exiger des employés qu'ils suivent périodiquement une formation et renforcer, à l'échelle de l'entreprise, l'attention portée à une bonne hygiène en matière de cybersécurité, telle que l'utilisation de mots de passe complexes et l'authentification multifactorielle, ainsi que la sensibilisation à l'hameçonnage et à d'autres formes de cyberattaques.