CSA/ACVM Canadian Securities Administrators | Autorités canadiennes en valeurs mobilières

Avis multilatéral 51-347 du personnel des ACVM
Information sur les risques et les incidents liés à la cybersécurité

Le 19 janvier 2017

Introduction

Les Autorités canadiennes en valeurs mobilières (**ACVM**) ont fait de la cybersécurité une priorité dans leur plan d'affaires 2016-2019. Elles ont publié, le 27 septembre dernier, l'Avis 11-332 du personnel des ACVM, *Cybersécurité* (l'**Avis 11-332**) pour insister sur l'importance des risques liés à la cybersécurité pour les émetteurs, les personnes inscrites et les entités réglementées et informer les parties intéressées de leurs projets récents et à venir. On y indiquait que des membres des ACVM examineraient l'information communiquée par certains grands émetteurs pour en analyser le contenu sous l'angle des risques liés à la cybersécurité et des cyberattaques.

Récemment, le personnel des ACVM a donc passé en revue l'information obtenue auprès des entreprises constituant l'Indice composé S&P/TSX concernant les risques liés à la cybersécurité et les cyberattaques. Le personnel de la British Columbia Securities Commission, de la Commission des valeurs mobilières de l'Ontario et de l'Autorité des marchés financiers (le **personnel** ou **nous**) publie le présent avis (l'**avis du personnel**) afin de présenter les conclusions de son examen et de faire part aux émetteurs assujettis de ses attentes en matière d'information.

Par le passé, le personnel de certains membres des ACVM a effectué des examens de l'information fournie sur la cybersécurité, notamment dans le cadre de sa collaboration au rapport de l'Organisation internationale des commissions de valeurs (**OICV**) sur la cybersécurité dans les marchés des valeurs mobilières (le **rapport de l'OICV**)[1]. Le présent avis du personnel expose cependant les résultats d'un examen des émetteurs ayant une plus grande portée. Nous avons entrepris cet examen parce que nous estimons que les émetteurs de tous les secteurs peuvent être exposés à des risques liés à la cybersécurité, bien qu'ils le soient de différentes façons.

Examen limité à un sujet précis

Nous avons passé en revue les derniers documents annuels déposés par les 240 entreprises constituant l'Indice composé S&P/TSX[2], dont les notices annuelles, les rapports de gestion, les circulaires de sollicitation de procurations ainsi que d'autres documents, comme les déclarations de changement important et les communiqués.

---

[1] Le rapport de l'OICV sur la cybersécurité dans les marchés des valeurs mobilières est accessible à l'adresse suivante :
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

[2] Au 7 juillet 2016.

Nous cherchions à savoir si et comment les émetteurs avaient abordé les questions de cybersécurité dans l'information sur les facteurs de risque, notamment si elle décrivait les répercussions possibles d'une cyberattaque sur leurs activités, le type d'information importante pouvant ainsi être exposée et communiquait l'identité du responsable de la stratégie de l'émetteur en matière de cybersécurité. Nous cherchions aussi de l'information sur les cyberincidents qui se seraient produits.

Information sur les facteurs de risque

Information sur les risques liés à la cybersécurité

Dans le cadre de notre examen, nous avons constaté que 146 émetteurs sur 240, soit 61 %, avaient traité de cybersécurité dans l'information sur les facteurs de risque.

De façon générale, les émetteurs ont indiqué que leur dépendance envers les systèmes de technologie de l'information les rendait vulnérables aux atteintes à la cybersécurité. Des émetteurs d'une grande diversité de secteurs ont reconnu que la cybersécurité représentait un risque important pour leurs activités.

Nous signalons également que peu d'émetteurs ont fourni de l'information sur leur vulnérabilité particulière aux cyberincidents. Par exemple, certains de ces émetteurs ont cité le secteur au sein duquel ils évoluent, les actifs précis détenus, la nature de leurs activités ou leur qualité d'entrepreneurs du gouvernement comme des facteurs augmentant la probabilité d'être la cible de cybersurveillance ou d'une cyberattaque orchestrée par des cybercriminels, des concurrents industriels ou des acteurs gouvernementaux. D'autres ont indiqué que leurs systèmes de technologie de l'information s'appuyaient sur une ancienne technologie et fonctionnaient avec un niveau minimal de soutien.

Certains émetteurs ont également abordé le risque que des tiers les exposent à des problèmes de cybersécurité. Les atteintes à la sécurité de tiers, l'insuffisance de l'expertise en cybersécurité et des mesures de protection de tiers partenaires et la défaillance ou l'arrêt des services de technologie de l'information de tiers auxquels se fie l'émetteur font partie de ces risques.

Information sur les répercussions possibles des cyberincidents

Les émetteurs ayant exposé la dépendance de leurs activités envers les systèmes de technologie de l'information ont indiqué que les perturbations attribuables aux cyberincidents pouvaient avoir des répercussions négatives sur leurs activités, leurs résultats d'exploitation et leur situation financière.

Les répercussions possibles suivantes d'un tel incident, mentionnées à plusieurs reprises, étaient communes à une variété d'émetteurs de différents secteurs :

- l'atteinte à la confidentialité des renseignements sur un client ou un salarié;
- l'accès non autorisé à de l'information exclusive ou sensible;
- la destruction ou la corruption de données;
- la perte de revenus en raison d'une perturbation des activités, l'engagement de coûts pour corriger la situation;

- des litiges, des amendes et la responsabilité en cas de non-respect des lois sur la protection de la vie privée et la sécurité de l'information;
- des enquêtes réglementaires et une plus grande surveillance des autorités de réglementation;
- l'augmentation des primes d'assurance;
- une atteinte à la réputation venant ébranler la confiance des clients et des investisseurs;
- une diminution de l'avantage concurrentiel et des incidences négatives sur les occasions futures;
- l'efficacité du contrôle interne à l'égard de l'information financière.

Parmi les répercussions possibles propres à leurs activités ou à leur secteur relevées par les émetteurs, on comptait notamment :

- des retards opérationnels, comme des arrêts de la production ou des interruptions dans des usines et des services publics;
- l'incapacité à gérer la chaîne d'approvisionnement;
- l'incapacité à traiter les opérations des clients ou à servir autrement les clients;
- des perturbations dans la gestion des stocks;
- la perte de données provenant des activités de recherche et de développement;
- la dévaluation de la propriété intellectuelle.

Information sur la gouvernance et l'atténuation des risques liés à la cybersécurité

Nous avons examiné si les émetteurs avaient indiqué avoir confié à quelqu'un la responsabilité de leur stratégie en matière de cybersécurité et, le cas échéant, son identité. Nous avons constaté que 31 émetteurs, soit 20 %, avaient abordé la cybersécurité dans l'information communiquée et indiqué la personne, le groupe ou le comité responsable.

Les émetteurs ont le plus souvent mentionné le comité d'audit comme responsable de la surveillance des risques liés à la cybersécurité, souvent en collaboration avec la direction. Certains ont indiqué qu'un comité de gestion du risque était chargé de surveiller et de gérer les risques, dont ceux liés à la cybersécurité. Le conseil d'administration et la direction, considérés comme un tout, ont aussi été mentionnés, alors que quelques émetteurs ont précisé que le chef des finances ou le chef des technologies de l'information était chargé de surveiller les risques liés à la cybersécurité.

Certains émetteurs ont mentionné que des contrôles tels qu'un plan de reprise après sinistre et le contrôle des accès non autorisés avaient été mis en place. Peu d'émetteurs ont indiqué détenir une assurance contre les cyberincidents, certains ayant précisé que leur couverture pourrait être insuffisante pour de tels incidents.

Indications du personnel sur l'information à fournir sur les facteurs de risque

De façon générale, les émetteurs devraient se concentrer sur l'information importante et propre à leur situation et éviter les phrases toutes faites. Si nous reconnaissons que l'exposition aux risques liés à la cybersécurité est commune à l'ensemble des émetteurs de chacun des secteurs, les émetteurs devraient garder à l'esprit que l'information sur les facteurs de risque vise notamment à permettre aux lecteurs de distinguer un émetteur d'un autre, au sein d'un même

secteur ou dans l'ensemble, sur les plans du niveau d'exposition et de préparation et en fonction de l'incidence du risque sur lui.

Comme les émetteurs sont de plus en plus tributaires des technologies d'information pour exercer leurs activités, et que les cyberattaques gagnent en fréquence et en complexité, nous nous attendons à ce qu'ils se penchent sur les façons dont ils y seront vraisemblablement exposés et sur les formes qu'elles prendront.

Nous reconnaissons que tous les émetteurs peuvent faire l'objet d'une cyberattaque. Cependant, les émetteurs de certains secteurs peuvent être exposés à des risques liés à la cybersécurité pour des motifs différents de ceux des émetteurs d'autres secteurs, et à des degrés différents. Ainsi, la vulnérabilité d'un émetteur offrant directement des services aux consommateurs diffère de celle de l'émetteur qui détient de la propriété intellectuelle stratégique ou exploite des infrastructures. Les conséquences d'une cyberattaque peuvent varier grandement d'un émetteur à l'autre.

Comme il en était question dans l'Avis 11-332, les membres des ACVM s'attendent à ce que les émetteurs fournissent de l'information aussi détaillée et propre à leur situation que possible, dans la mesure où ils ont établi que le risque lié à la cybersécurité était important. L'importance relative dans les cas de risques liés à la cybersécurité s'articule autour d'une analyse de la probabilité qu'une atteinte survienne et de l'ampleur prévue de son incidence.

Puisque nous nous attendons à ce que les émetteurs indiquent des risques précis et non des risques généraux communs à l'ensemble d'entre eux, l'information sur les risques liés à la cybersécurité devrait être adaptée à leur situation. En revanche, ils n'ont pas à divulguer des détails sur leur stratégie en matière de cybersécurité ou leur vulnérabilité aux cyberattaques qui seraient sensibles ou pourraient compromettre leur cybersécurité.

Dans l'établissement de leur information, les émetteurs sont invités à tenir compte des facteurs soulevés par l'OICV. Ils devraient prendre en compte les raisons pour lesquelles ils pourraient être exposés à une atteinte à la cybersécurité, la source et la nature des risques, les conséquences éventuelles d'une cyberatteinte, le caractère adéquat des mesures préventives ainsi que les cyberincidents importants antérieurs et leurs effets sur leurs risques liés à la cybersécurité. Ils devraient aussi aborder la façon dont ils comptent atténuer les risques, notamment le maintien ou non d'une couverture d'assurance à l'égard des cyberattaques et, le cas échéant, son importance, ou leur dépendance envers des tiers experts pour leur stratégie en matière de cybersécurité ou la mise en place de mesures correctives à la suite des cyberattaques subies ou en prévision de celles à venir. Il est aussi pertinent d'aborder les questions de gouvernance, y compris d'indiquer le nom du comité ou de la personne responsable de leur stratégie en matière de cybersécurité et d'atténuation des risques. Nous invitons les émetteurs à consulter le chapitre 2 du rapport de l'OICV.

Enfin, nous nous attendons à ce que les émetteurs tenus d'établir et de maintenir des contrôles et des procédures en vertu du *Règlement 52-109 sur l'attestation de l'information présentée dans les documents annuels et intermédiaires des émetteurs* les appliquent aux cyberincidents ciblés pour s'assurer qu'ils soient communiqués à la direction et que la décision de les déclarer et, le cas échéant, quant à l'information à fournir, soit prise rapidement.

Information sur les cyberincidents

Si certains émetteurs ont signalé dans l'information sur les facteurs de risque avoir déjà fait l'objet de cyberattaques, aucun émetteur échantillonné n'a indiqué que ces incidents étaient importants. Un seul émetteur échantillonné a publié un communiqué suivant une atteinte à la protection de ses données qui s'est traduite par la divulgation de renseignements confidentiels. Or, il n'a pas déposé de déclaration de changement important en lien avec cet incident.

Nous signalons que certains émetteurs ont indiqué dans leurs documents d'information continue avoir déjà fait l'objet d'atteintes à la cybersécurité, mais que ces incidents n'étaient pas importants.

Indications du personnel sur la déclaration d'incidents

Nous comprenons que la législation sur la protection des renseignements personnels ou toute autre législation peut exiger que les émetteurs déclarent à certaines personnes les atteintes à la cybersécurité dans certains cas, ou les en avisent, mais ces obligations diffèrent de celles prévues par la législation en valeurs mobilières.

Lorsqu'il évalue s'il doit déclarer un cyberincident et, le cas échéant, le moment de le faire, l'émetteur doit déterminer s'il s'agit d'un fait ou d'un changement important devant être communiqué conformément à la législation en valeurs mobilières. Il devrait consulter les indications présentées dans l'*Instruction générale 51-201 : Lignes directrices en matière de communication de l'information* et peut aussi se reporter au paragraphe *f* de la partie 1 de l'Annexe 51-102A1, *Rapport de gestion* et au paragraphe *e* de la partie 1 de l'Annexe 51-102A2, *Notice annuelle* du *Règlement 51-102 sur les obligations d'information continue*.

Nous sommes conscients qu'il n'existe aucun critère de démarcation et que le seuil quantitatif ou qualitatif auquel une atteinte à la cybersécurité devient importante peut varier d'un émetteur et d'un secteur à l'autre, selon la situation de l'émetteur ainsi que le type d'incidence et l'ampleur des conséquences.

L'importance relative est fonction de l'analyse contextuelle de l'incident. Si une cyberattaque isolée n'est pas nécessairement importante, une série d'incidents ou des incidents mineurs fréquents peuvent être importants à la lumière du niveau et du type de perturbation causée. L'incidence d'une attaque par déni de service distribué ou d'un rançongiciel différerait de celle d'une atteinte à la cybersécurité visant à obtenir des renseignements sur un client. Les éléments d'information à fournir, que ce soit dans l'information sur les facteurs de risque, l'information financière ou les rapports d'incidents de l'émetteur, dépendent des circonstances de l'incident.

Le moment où l'information sur les cyberincidents importants est fournie constitue un facteur important. Nous sommes conscients que ce type d'incident peut n'être détecté que beaucoup plus tard par la suite, et qu'il peut être long d'en évaluer les conséquences de façon approfondie. La détermination de l'importance d'un incident est un processus dynamique se déroulant tout au long des phases de détection et d'évaluation de l'incident et de mise en place des mesures correctives.

Comme l'indique l'Avis 11-332, nous nous attendons à ce que les émetteurs précisent dans tout plan de reprise après une cyberattaque la façon dont l'importance de celle-ci serait évaluée pour établir si de l'information doit être rendue publique à son sujet et, le cas échéant, à quel moment et de quelle façon. Dans le cadre de l'évaluation, les émetteurs devraient tenir compte des répercussions sur leurs activités, leur réputation, leurs clients, leurs salariés et leurs investisseurs. L'émetteur qui décide de déclarer un cyberincident pourrait envisager d'en communiquer les répercussions et les coûts prévus.

Prochaines étapes

Le personnel compte poursuivre son examen de l'information sur les risques liés à la cybersécurité et les cyberincidents, surveiller les tendances dans l'information à fournir et analyser l'étendue de l'information contenue dans les déclarations sur ce type d'incident et le moment où elle est communiquée.

Questions

Pour toute question, veuillez vous adresser à l'une des personnes suivantes :

Georgia Koutrikas
Analyste, Financement des sociétés
Autorité des marchés financiers
514 395-0337, poste 4393
georgia.koutrikas@lautorite.qc.ca

Martin Latulippe
Directeur, Information continue
Autorité des marchés financiers
514 395-0337, poste 4331
martin.latulippe@lautorite.qc.ca

Matthew Au
Senior Accountant, Corporate Finance Branch
Commission des valeurs mobilières de
l'Ontario
416 593-8132
mau@osc.gov.on.ca

Allan Lim
Manager, Corporate Finance
British Columbia Securities Commission
604 899-6780
alim@bcsc.bc.ca