CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Alerte info

INFORMATION D'ENTREPRISE

AVRIL 2017

Risques et incidents liés à la cybersécurité : Réévaluer vos pratiques de communication de l'information

Dans le contexte d'affaires étroitement interconnecté et en constante évolution d'aujourd'hui, les organisations sont amenées à exercer divers aspects de leurs activités commerciales dans le « cyberespace ». Le cyberespace est l'endroit où les particuliers et les organisations établissent une présence électronique et mènent des activités virtuelles, en échangeant des renseignements, des produits et des services sur Internet[1]. Bien que l'exercice d'activités dans le cyberespace comporte des avantages, cette pratique rend aussi les organisations vulnérables aux cyberattaques de criminels dont les conséquences désastreuses vont au-delà du vol d'information et des pertes financières[2].

La cybersécurité se veut une réponse aux risques liés au cyberespace et désigne, de façon générale, les processus et les pratiques en place pour protéger les systèmes et les données informatiques contre les menaces du cyberespace. Étant donné les incidences considérables sur la réputation et sur les plans opérationnel, financier, légal et réglementaire des récentes atteintes hautement médiatisées à l'intégrité des données, les investisseurs souhaitent de plus en plus comprendre l'exposition d'une organisation aux risques liés à la cybersécurité ainsi que les politiques, les processus et les contrôles connexes en place pour atténuer ces risques.

1 ***Actualités Administrateurs :*** **« Risques liés à la cybersécurité – Questions que les administrateurs devraient poser »**

2 Dans un rapport publié par le conseil d'administration de l'Organisation internationale des commissions de valeurs (OICV), les cyberattaques sont définies comme étant des tentatives de compromettre la confidentialité, l'intégrité et la disponibilité de données ou de systèmes informatiques. ***Cyber Security in Securities Markets – An International Perspective***, avril 2016

Il faut exercer beaucoup de jugement pour déterminer si des risques et des incidents liés à la cybersécurité sont importants et doivent être communiqués conformément aux obligations d'information existantes. De par leur nature, les risques liés au cyberespace sont très complexes. La nature et l'étendue des informations à fournir sur l'exposition aux risques liés à la cybersécurité varieront, en pratique, de façon importante d'une entité à l'autre en fonction de sa situation propre. Il y a de nombreux contextes dans lesquels les entreprises sont tenues, conformément aux obligations d'information existantes, de fournir des informations sur les risques liés à la cybersécurité. En voici des exemples :

- **Notice annuelle :** Un émetteur assujetti doit indiquer les facteurs de risque, y compris les risques généraux inhérents à la nature des activités de la société et les autres questions susceptibles d'influer sur la décision d'un investisseur d'acquérir des titres de la société.

- **Rapport de gestion :** Le rapport de gestion doit traiter, entre autres choses, des tendances et des risques importants qui ont déjà eu ou dont il est raisonnable de croire qu'ils auront une incidence sur les états financiers.

- **Déclaration de changement important :** Lorsqu'un changement important survient dans les affaires d'un émetteur assujetti, ce dernier doit immédiatement publier et déposer un nouveau communiqué indiquant la nature et la substance du changement. Il doit également déposer une déclaration de changement important dès que possible dans les 10 jours suivant le changement.

- **États financiers :** Les risques et les incidents liés à la cybersécurité peuvent également influer sur les informations à fournir dans les états financiers (p. ex., les coûts et les autres conséquences liées aux cyberincidents importants).

En plus de communiquer l'information exigée conformément à la réglementation sur les valeurs mobilières, un grand nombre d'émetteurs cherchent à cerner et à aborder d'autres questions d'intérêt pour leurs parties intéressées (p. ex., dans les documents complémentaires, que l'on peut consulter sur leur site Web).

Avis 51-347 du personnel des ACVM

Les Autorités canadiennes en valeurs mobilières (ACVM) ont publié, le 19 janvier 2017, l'**Avis multilatéral 51-347 du personnel des ACVM *Information sur les risques et les incidents liés à la cybersécurité*** (l'Avis 51-347 du personnel des ACVM ou l'Avis), qui présente les attentes en matière d'information de la part des émetteurs assujettis relativement aux risques liés à la cybersécurité et aux cyberincidents.

La présente *Alerte info* fait le point sur l'Avis 51-347 du personnel des ACVM et présente les enjeux liés à la communication de l'information sur la cybersécurité. Ce bulletin ne traite pas des pratiques et des procédures sous-jacentes relatives à la cybersécurité, ni ne tente de fournir des conseils sur la manière de se conformer à la réglementation sur les valeurs mobilières. La question de savoir si les informations fournies dans les documents déposés

en vertu de la réglementation sur les valeurs mobilières sont conformes aux exigences pertinentes est essentiellement une question juridique et doit donc être analysée attentivement. La présente *Alerte info* vise à fournir des informations générales à titre indicatif seulement. Elle ne saurait se substituer à l'examen de l'Avis 51 347 du personnel des ACVM, ni à des services-conseils.

Principales constatations

L'Avis est fondé sur un examen de l'information communiquée sur les risques liés à la cybersécurité et les cyberincidents. L'examen est fondé en partie sur le rapport intitulé ***Cyber Security in Securities Markets – An International Perspective***, publié par le conseil d'administration de l'Organisation internationale des commissions de valeurs (OICV) en avril 2016 (le rapport de l'OICV). Le personnel des ACVM a passé en revue les documents déposés par les 240 entreprises constituant l'indice composé S&P/TSX et a cherché à savoir ce qui suit :

- 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;
- l'identité du responsable de la stratégie de l'émetteur en matière de cybersécurité;
- l'information sur les cyberincidents qui se seraient produits.

Information sur les risques liés à la cybersécurité

Le personnel des ACVM a constaté que 61 % des émetteurs ayant fait l'objet d'un examen avaient traité de cybersécurité dans l'information sur les facteurs de risque et avaient reconnu que leur dépendance envers les systèmes de technologie de l'information les rendait vulnérables aux atteintes à la cybersécurité. Toutefois, 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, leur qualité d'entrepreneurs du gouvernement ou la nature de leurs systèmes de technologie de l'information. Certains émetteurs ont abordé le risque que des tiers les exposent à des problèmes de cybersécurité.

Information sur les répercussions possibles des cyberincidents

Les émetteurs ayant traité de cybersécurité dans leur information sur les facteurs de risque ont également précisé 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 mentionnées par une variété d'émetteurs de différents secteurs comprenaient notamment ce qui suit :

- l'atteinte à la confidentialité des renseignements sur un client ou un employé;
- 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;
- 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

Le personnel des ACVM a constaté que 20 % des émetteurs qui avaient abordé la cybersécurité dans l'information communiquée ont indiqué la personne, le groupe ou le comité responsable de la surveillance des risques liés à la cybersécurité. Ces émetteurs ont le plus souvent mentionné le comité d'audit comme responsable de cette surveillance, souvent en collaboration avec la direction.

D'autres émetteurs ont mentionné le comité de gestion des risques, le conseil d'administration et la direction, considérés comme un tout, ou des personnes telles que le chef des finances ou le chef des technologies de l'information. Certains émetteurs ont indiqué qu'un plan de reprise après sinistre ou qu'un contrôle des accès non autorisés avait été mis en place. Toutefois, peu d'émetteurs ont indiqué s'ils détenaient ou non une couverture d'assurance suffisante contre de tels incidents.

Indications du personnel des ACVM

Généralités

Comme le suggère l'Avis, les émetteurs devraient se concentrer sur l'information importante et propre à leur situation et éviter les phrases toutes faites. Les formulations propres à l'entité devraient 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. L'importance relative s'articule autour d'une analyse de la probabilité qu'une atteinte survienne et de l'ampleur prévue de son incidence. Le personnel des ACVM ne s'attend pas à ce que les émetteurs divulguent des détails sur leur stratégie en matière de cybersécurité ou leur vulnérabilité aux cyberattaques qui seraient sensibles ou pourraient compromettre leur cybersécurité.

Risque et exposition

La communication d'informations appropriées peut porter sur les raisons pour lesquelles un émetteur pourrait être exposé à une atteinte à la cybersécurité, sur la source et la nature des risques, sur les conséquences éventuelles d'une atteinte et sur le caractère adéquat des mesures préventives. Les informations peuvent également porter sur les cyberincidents importants antérieurs et leurs effets sur les risques liés à la cybersécurité de l'émetteur.

Atténuation des risques

Les émetteurs devraient aborder la façon dont ils comptent atténuer les risques liés à la cybersécurité, notamment leur degré de 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. Les émetteurs devraient aussi aborder les questions de gouvernance, y compris indiquer le nom du comité ou de la personne responsable de leur stratégie en matière de cybersécurité et d'atténuation des risques. Les informations peuvent également porter sur la nature et l'étendue de la couverture d'assurance pertinente. Comme l'indique l'Avis, le rapport de l'OICV constitue une référence importante en matière d'évaluation du caractère adéquat des informations fournies.

Communication de l'information en temps opportun

À la suite d'un cyberincident, 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. Encore une fois, il n'existe aucun critère de démarcation aux fins de cette évaluation; le seuil auquel une atteinte à la cybersécurité devient importante peut varier d'un émetteur et d'un secteur à l'autre. Comme le reconnaît l'Avis, il peut être long d'évaluer les conséquences d'un cyberincident (et par conséquent, son importance relative) de façon approfondie. 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.

Dans tout plan de reprise après une cyberattaque, le personnel des ACVM s'attend à ce que les émetteurs précisent la façon dont l'importance relative 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.

Quelques questions pour la direction et le conseil d'administration

Les questions clés suivantes peuvent aider la direction et le conseil d'administration des émetteurs assujettis lors de l'évaluation de leurs pratiques en matière de communication des risques liés à la cybersécurité :

1. Avons-nous documenté le cyberespace dans lequel nos partenaires commerciaux et nous-mêmes exerçons nos activités et en avons-nous une bonne compréhension?

2. Avons-nous évalué si l'information que nous communiquons sur les risques liés à la cybersécurité, compte tenu des considérations énoncées dans l'Avis du personnel des ACVM, est adéquate dans l'ensemble?

3. Avons-nous évalué séparément, pour chacun de nos principaux documents de communication périodique d'information, quelles informations doivent être communiquées à propos des risques liés à la cybersécurité sur les plans opérationnel, financier et réglementaire? Avons-nous des procédures en place pour revoir régulièrement ces informations?

4. Avons-nous établi des procédures internes pour évaluer l'importance relative des atteintes à la cybersécurité ou d'autres incidents?

5. Avons-nous évalué l'information sur les risques liés à la cybersécurité communiquée par d'autres sociétés de notre secteur ou dans des circonstances semblables?

6. Avons-nous pris des mesures pour comprendre les préoccupations que nos investisseurs peuvent avoir au sujet de notre exposition à des risques liés à la cybersécurité et la façon dont nous devrions aborder ces préoccupations dans l'information que nous communiquons?

7. La conception de nos contrôles et de nos procédures de communication de l'information comprend-elle des processus permettant de s'assurer que les cyberincidents sont communiqués à la direction et que les décisions qui en découlent, quant à l'information à fournir, sont prises rapidement?

8. Savons-nous de quelle manière nos auditeurs externes tiennent compte des risques liés à la cybersécurité dans la planification et la réalisation de leur audit?

9. Sommes-nous convaincus qu'une attention appropriée est portée aux risques liés à la cybersécurité et à leur atténuation dans notre structure de gouvernance? Les responsabilités quant à la surveillance de ces risques et à leur atténuation sont-elles clairement définies?

   La personne ou le groupe responsable de la surveillance des risques liés à la cybersécurité consacre-t-il suffisamment de temps à ces questions et reçoit-il les commentaires, le soutien et les ressources appropriés de la part de notre organisation dans son ensemble? Tous ces éléments sont-ils suffisamment clairs dans l'information que nous communiquons?

10. Avons-nous élaboré des mesures clés de performance internes quant à notre façon de surveiller, de détecter et de gérer les risques liés à la cybersécurité? Le cas échéant, devrions-nous rendre ces mesures publiques?

Autres ressources

- **Avis 11-326 du personnel des ACVM, *Cybersécurité***
- **Avis 11-332 du personnel des ACVM, *Cybersécurité***
- ***Actualités Administrateurs* : « Risques liés à la cybersécurité – Questions que les administrateurs devraient poser »**

Merci de faire parvenir vos commentaires sur le présent bulletin *Alerte info*, ou vos suggestions pour les prochains bulletins, à :

Rosemary McGuire, CPA, CA
Directrice de projets, Information financière et marchés financiers
Recherche, orientation et soutien
Comptables professionnels agréés du Canada
277, rue Wellington Ouest
Toronto (Ontario) M5V 3H2
Courriel : **rmcguire@cpacanada.ca**

AVERTISSEMENT
La présente publication, préparée par Comptables professionnels agréés du Canada (CPA Canada), fournit des indications ne faisant pas autorité.

CPA Canada et les auteurs déclinent toute responsabilité ou obligation pouvant découler, directement ou indirectement, de l utilisation ou de l application de cette publication.

DROITS D'AUTEUR
Copyright © 2017 Comptables professionnels agréés du Canada

Tous droits réservés. Cette publication est protégée par des droits d auteur et ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise de quelque manière que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode) sans autorisation écrite préalable.

Pour obtenir des renseignements concernant l obtention de cette autorisation, veuillez écrire à **permissions@cpacanada.ca**