CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Alerte info

COMMUNICATION DE L'INFORMATION D'ENTREPRISE

JUIN 2018

Cybersécurité – Établir un programme de gestion des risques et continuer de réévaluer les pratiques de communication de l'information

Contexte

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. Bien que l'exercice d'activités dans le cyberespace comporte de nombreux avantages, cette pratique rend aussi les organisations vulnérables aux cyberattaques[1]. Ces menaces planent sur toutes les organisations, y compris les entreprises ayant une obligation d'information du public, les entreprises à capital fermé, les organismes sans but lucratif, les entités liées à une autorité publique et d'autres entités.

Le terme « cybersécurité » désigne, de façon générale, les processus et les pratiques en place pour protéger les systèmes et les données informatiques contre les menaces prenant leur origine dans le cyberespace. L'obligation de rendre des comptes à l'égard des différents aspects de la cybersécurité peut revenir à de nombreuses fonctions d'une organisation, parmi lesquelles on retrouve souvent le service des finances. Étant donné les répercussions considérables que

1 Dans un rapport publié par le conseil d'administration de l'Organisation internationale des commissions de valeurs (OICV), les cyberattaques sont définies comme étant [TRADUCTION] « 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.

des cas récents et hautement médiatisés d'atteinte à la protection des données ont eues au chapitre de la réputation et sur les plans opérationnel, financier, légal et réglementaire, les investisseurs et les autres parties prenantes sont de plus en plus intéressés à comprendre l'exposition d'une organisation aux risques liés à la cybersécurité ainsi que les politiques, les processus et les contrôles connexes qu'elle a mis en place pour atténuer ces risques. Dans son budget de février 2018, le gouvernement fédéral a alloué près de 500 millions de dollars sur cinq ans à la cybersécurité, notamment pour la création du Centre canadien pour la cybersécurité et d'une Unité nationale de coordination de la lutte contre la cybercriminalité.

Objet de la présente *Alerte info*

Le 19 janvier 2017, les Autorités canadiennes en valeurs mobilières (ACVM) ont publié 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 »), qui présente les attentes envers les émetteurs assujettis en ce qui concerne l'information sur les risques liés à la cybersécurité et les cyberincidents. Dans notre *Alerte info* d'avril 2017, « **Risques et incidents liés à la cybersécurité : Réévaluer vos pratiques de communication de l'information** », nous faisions le point sur l'Avis 51-347 du personnel des ACVM et sur les enjeux liés à la communication de l'information sur la cybersécurité.

La présente publication s'ajoute à notre *Alerte info* d'avril 2017 à deux égards :

- elle énonce les éléments que la direction de toutes les entités doit prendre en considération lors de l'élaboration d'un programme de gestion des risques liés à la cybersécurité;
- elle fait une mise au point sur le contexte actuel en matière de communication de l'information pour les émetteurs inscrits et assujettis, y compris les indications récentes publiées par les ACVM et par la Securities and Exchange Commission (SEC) des États-Unis.

Élaboration d'un programme de gestion des risques liés à la cybersécurité

En 2017, l'American Institute of Certified Public Accountants (AICPA) des États-Unis a élaboré un cadre d'information qui aide les organisations à communiquer des informations pertinentes et utiles concernant l'efficacité de leurs programmes de gestion des risques liés à la cybersécurité[2]. L'AICPA a aussi mis en ligne **System and Organization Controls (SOC) for Cybersecurity (SOC for Cybersecurity): Reporting on an Entity's Cybersecurity Risk Management Program and Controls** pour permettre aux CPA d'examiner ces informations et de faire rapport à leur sujet[3]. Le rapport d'examen de la gestion des risques liés à la cybersécurité comprend les trois composantes clés qui suivent :

2 www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityfororganizations.html

3 CPA Canada élabore actuellement un guide sur les rapports délivrés à l'égard du programme de gestion des risques et des contrôles d'une entité en matière de cybersécurité (CSS Cybersécurité) adapté aux Normes canadiennes d'audit. Il sera bientôt mis en vente sur la boutiqueCPA.

- une description narrative du programme de gestion des risques liés à la cybersécurité de l'entité, préparée par la direction et englobant des renseignements sur la façon dont l'entité identifie ses informations les plus sensibles et gère les risques liés à la cybersécurité qui la menacent, ainsi que sur les politiques et processus clés mis en œuvre et exploités en matière de sécurité pour protéger les actifs informationnels de l'entité contre ces risques[4];
- une assertion de la direction indiquant si la description est présentée conformément aux critères établis par l'AICPA et si les contrôles du programme ont été efficaces pour atteindre les objectifs de l'entité en matière de cybersécurité compte tenu des critères de contrôle de l'AICPA;
- l'opinion d'un CPA sur la description de la direction et sur l'assertion de la direction en ce qui concerne l'efficacité des contrôles contenus dans le programme de gestion des risques liés à la cybersécurité.

L'AICPA a publié un exemple illustratif d'un tel rapport de gestion des risques liés à la cybersécurité, y compris les critères servant à évaluer la description de la direction et l'efficacité des contrôles établis pour atteindre les objectifs de l'entité en matière de cybersécurité, offrant ainsi un point de référence utile pour la direction de toutes les entités en vue de la conception et de la mise en place d'un programme de gestion des risques liés à la cybersécurité[5]. L'annexe de la présente publication énonce un certain nombre de questions que doivent se poser la direction et le conseil d'administration dans le contexte de l'élaboration d'un programme de gestion des risques liés à la cybersécurité selon les critères de description et l'exemple illustratif de l'AICPA.

Indications récentes des ACVM et de la SEC concernant les risques liés à la cybersécurité

Le 19 octobre 2017, les ACVM ont publié l'**Avis 33-321 du personnel des ACVM, *Cybersécurité et médias sociaux*** (l'« Avis 33-321 du personnel des ACVM »), qui résume les résultats du sondage sur les pratiques en matière de cybersécurité et de médias sociaux des sociétés inscrites à titre de gestionnaires de fonds d'investissement, de gestionnaires de portefeuille et de courtiers sur le marché dispensé. L'Avis 33-321 du personnel des ACVM fournit à ces sociétés des indications en proposant des politiques et des procédures sur les pratiques en matière de cybersécurité et de médias sociaux.

Le 26 février 2018, la SEC a publié des indications interprétatives pour aider les sociétés ouvertes à préparer les informations à fournir sur les risques liés à la cybersécurité et sur les cyberincidents[6]. Le contenu de ces indications est semblable, à de nombreux égards, à celui de l'Avis 51-347 du personnel des ACVM. Même pour les émetteurs assujettis canadiens qui ne sont pas inscrits aux États-Unis, les indications de la SEC fournissent un point de référence

4 Les critères de description de l'AICPA que doit utiliser la direction pour concevoir et décrire son programme de gestion des risques liés à la cybersécurité peuvent être consultés à l'adresse **www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/description-criteria.pdf**.

5 Dans le lien suivant, la section 3 comprend un exemple illustratif de la description que doit faire la direction du programme de gestion des risques liés à la cybersécurité de l'entité : **www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/illustrative-cybersercurity-risk-management-report.pdf**.

6 **Release Nos. 33-10459; 34-82746 Commission Statement and Guidance on Public Company Cybersecurity Disclosures**.

supplémentaire pour déterminer si leurs informations et leurs pratiques sont adéquates sur une base continue. Par exemple, ces indications mettent davantage l'accent sur des questions pouvant avoir une incidence sur les états financiers, faisant ainsi ressortir que les cyberincidents sont susceptibles d'entraîner :

- des charges relatives aux investigations, à la notification des atteintes à la protection des données, aux litiges et aux mesures correctives, y compris les coûts des services juridiques et autres services professionnels;
- la perte de produits, la nécessité d'offrir des incitations aux clients et la perte de valeur des relations avec les clients en tant que valeur d'actif;
- des réclamations au titre des garanties, un bris de contrat, le rappel ou le remplacement de produits, l'indemnisation des contreparties et des hausses des primes d'assurance;
- la diminution des flux de trésorerie futurs et la dépréciation du capital intellectuel, des immobilisations incorporelles et d'autres actifs;
- la comptabilisation de passifs ou l'augmentation des coûts de financement.

La SEC s'attend à ce que les systèmes d'information financière et de contrôle d'une société soient conçus de façon à fournir une assurance raisonnable que les informations concernant la portée et l'ampleur des répercussions financières d'un cyberincident seront intégrées dans ses états financiers en temps opportun, à mesure qu'elles seront disponibles. Les émetteurs assujettis canadiens qui sont tenus d'établir et de maintenir un contrôle interne à l'égard de l'information financière (CIIF), et dont les dirigeants signataires sont tenus de traiter de l'évaluation de l'efficacité du CIIF dans leur attestation des documents annuels, devraient probablement aussi considérer les aspects décrits ci-dessus comme des facteurs de risque aux fins de la conception de leur CIIF et de la détermination des moyens d'en évaluer l'efficacité.

Annexe

Questions que la direction doit prendre en considération lorsqu'elle élabore un programme de gestion des risques liés à la cybersécurité

Les questions suivantes se fondent sur la description du programme de gestion des risques contenue dans l'exemple de rapport de gestion des risques liés à la cybersécurité de l'AICPA. Les questions soulevées ne sont pas exhaustives.

Nature des affaires et des activités

Avons-nous adéquatement évalué et documenté la nature de nos affaires et de nos activités, y compris les principaux produits que nous vendons ou services que nous fournissons, de même que les méthodes que nous utilisons aux fins de leur distribution?

Nature des informations à risque

Avons-nous évalué les principaux types d'informations sensibles que nous créons, recueillons, transmettons, utilisons ou entreposons et qui comportent des risques inhérents liés à la cybersécurité?

Objectifs du programme de gestion des risques liés à la cybersécurité

La direction a-t-elle établi, sous l'autorité du conseil d'administration, les principaux objectifs de notre programme de gestion des risques liés à la cybersécurité relativement à la disponibilité, à la confidentialité et à l'intégrité des données, de même qu'à l'intégrité de leur traitement, ainsi que le processus de maintien et d'approbation de ces objectifs pour toutes les unités et fonctions de l'entité?

Facteurs ayant un effet important sur les risques inhérents liés à la cybersécurité

Avons-nous identifié et documenté les facteurs ayant un effet important sur les risques inhérents liés à la cybersécurité, y compris :

- les caractéristiques de nos technologies, de nos types de connexion, de notre utilisation de fournisseurs de services et de nos modes de prestation?
- les caractéristiques de l'organisation et des utilisateurs?
- les changements environnementaux, technologiques et organisationnels ainsi que les autres changements nous concernant et touchant notre environnement?

Dans le cas des cyberincidents qui ont considérablement compromis l'atteinte de nos objectifs en matière de cybersécurité, avons-nous pleinement évalué et documenté la nature et l'étendue du cyberincident, le moment auquel il s'est produit, ainsi que la manière dont il a été résolu ou corrigé?

Structure de gouvernance des risques liés à la cybersécurité

Avons-nous établi des processus :

- visant à établir, à maintenir et à transmettre des valeurs d'éthique et d'intégrité pour soutenir le fonctionnement du programme de gestion des risques liés à la cybersécurité?
- concernant les grandes lignes de communication de l'information et de reddition de comptes en matière de cybersécurité?
- concernant la surveillance du programme par le conseil?

- visant à embaucher et à perfectionner des personnes et des entrepreneurs compétents, et à faire en sorte qu'ils rendent des comptes en ce qui a trait à leurs responsabilités en matière de cybersécurité?

Processus d'évaluation des risques liés à la cybersécurité

Avons-nous établi des processus visant :

- à identifier les risques liés à la cybersécurité de même que les changements environnementaux, technologiques, organisationnels et autres qui pourraient avoir un effet important sur notre programme de gestion des risques liés à la cybersécurité, y compris les exigences légales et réglementaires pertinentes?
- à évaluer les risques connexes pour l'atteinte de nos objectifs en matière de cybersécurité?
- à identifier, à évaluer et à gérer les risques associés aux fournisseurs et aux partenaires commerciaux?

Communications en matière de cybersécurité et qualité des informations sur la cybersécurité

Avons-nous établi un processus afin de communiquer à l'interne les informations pertinentes sur la cybersécurité qui sont nécessaires au fonctionnement de notre programme de gestion des risques liés à la cybersécurité, y compris :

- les objectifs, les attentes et les responsabilités en matière de cybersécurité?
- les seuils de communication des événements touchant la sécurité identifiés qui font l'objet d'une surveillance et d'une investigation, et dont il a été déterminé qu'il s'agissait de cyberincidents nécessitant une réponse, des mesures correctives ou les deux?

Surveillance du programme de gestion des risques liés à la cybersécurité

Avons-nous établi des processus visant :

- à effectuer des évaluations continues et périodiques de l'efficacité du fonctionnement des activités de contrôles clés et des autres composantes du contrôle interne ayant trait à la cybersécurité?
- à évaluer les menaces, les vulnérabilités et les déficiences des contrôles identifiées en ce qui a trait à la sécurité, et à les communiquer en temps opportun aux parties responsables de la prise de mesures correctives, y compris la direction et le conseil d'administration, au besoin?

Processus de contrôle liés à la cybersécurité

Avons-nous établi des processus visant :

- à élaborer une réponse à l'évaluation des risques, y compris la conception et la mise en place de processus de contrôle?
- à revoir notre infrastructure informatique et les caractéristiques de l'architecture de son réseau?
- à revoir les politiques et processus clés en matière de sécurité qui ont été mis en place et qui servent à traiter les risques liés à la cybersécurité auxquels nous sommes exposés, y compris ceux qui visent :
  - à prévenir les événements, intentionnels et non intentionnels, touchant la sécurité?
  - à détecter les événements touchant la sécurité, à identifier les incidents liés à la sécurité, à élaborer une réponse à ces incidents, et à mettre en place des activités pour atténuer les incidents identifiés en matière de sécurité et pour se remettre de tels incidents?
  - à gérer les capacités de traitement afin d'assurer la poursuite des activités en cas d'événements liés à la sécurité, à l'exploitation et à l'environnement?
  - à détecter et à atténuer les événements liés à l'environnement et à se remettre de tels événements, ainsi qu'à utiliser des procédures de sauvegarde pour assurer la disponibilité des systèmes?
  - à repérer les renseignements confidentiels lorsqu'ils sont reçus ou créés, à déterminer la période de conservation qui s'applique à ces renseignements, à les conserver pendant la période précisée et à les détruire à la fin de la période de conservation?

Autres ressources

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

Commentaires

Veuillez faire parvenir vos commentaires sur le présent numéro du bulletin *Alerte info*, ou vos suggestions pour les prochains numéros, à :

Dina Georgious, CPA, CA
Directrice de projets
Recherche, orientation et soutien
Comptables professionnels agréés du Canada
277, rue Wellington Ouest
Toronto (Ontario) M5V 3H2
Courriel : dgeorgious@cpacanada.ca