Quand le monde évolue à vitesse grand V, comment vos mesures de cybersécurité peuvent-elles suivre le rythme?

Rapport sur l'information relative à la cybersécurité

Mai 2020

Meilleure la question,
meilleure la réponse.
Pour un monde meilleur.

CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

EY
Travailler ensemble
pour un monde meilleur

Dans un monde où les cyberattaques sont inévitables, les conseils d'administration, les investisseurs, les autorités de réglementation et d'autres parties prenantes de la gouvernance s'intéressent de plus en plus à la façon dont les sociétés se protègent contre les menaces liées à la cybersécurité, planifient en fonction de ces menaces et y répondent.

Comme les menaces liées à la cybersécurité et à la protection des renseignements personnels deviennent de plus en plus complexes et de plus en plus répandues, les parties prenantes doivent passer au peigne fin les informations que les sociétés fournissent sur la cybersécurité dans les documents publics qu'elles déposent.

Afin d'informer les sociétés canadiennes sur les informations fournies actuellement, EY et Comptables professionnels agréés du Canada (CPA Canada) ont conjugué leurs efforts pour analyser les pratiques des sociétés ouvertes canadiennes en matière d'information sur la cybersécurité. Ce projet vient compléter les travaux du EY US Center for Board Matters qui, en 2018, a entrepris d'analyser l'information que communiquent les sociétés ouvertes américaines au sujet des risques liés à la cybersécurité et de la surveillance de ces risques.

Le projet canadien consiste à analyser les documents publics déposés en 2018 par les 60 sociétés à grande capitalisation les plus importantes inscrites à la Bourse de Toronto, afin de comprendre la nature et l'étendue de l'information fournie sur la cybersécurité dans les documents déposés auprès des autorités de réglementation, notamment les notices annuelles, les états financiers, les circulaires de la direction, les rapports de gestion et les déclarations de changement important, le cas échéant.

Pour de plus amples renseignements sur l'étendue et la méthode, consultez l'annexe.

Photo de couverture : Vincent Van Zalinge sur Unsplash

Principales observations

Même si bon nombre de sociétés ont indiqué que la cybersécurité était une question clé pour elles, le niveau de transparence et la quantité d'informations fournies varient selon les sociétés ouvertes canadiennes analysées. Nos principales constatations sont présentées ci-dessous.

Principales constatations

Communication des risques

98 %

des sociétés canadiennes ont mentionné la cybersécurité comme facteur de risque.

Surveillance exercée par le conseil

72 %

des sociétés canadiennes ont indiqué qu'au moins un comité du conseil est responsable des activités de surveillance liées à la cybersécurité.

Gestion des incidents liés à la cybersécurité

42 %

des sociétés canadiennes ont mentionné qu'elles misent sur des plans de réponse, de reprise après sinistre ou de poursuite des activités.

Cyberattaques

20 %

des sociétés canadiennes ont mentionné qu'elles avaient été la cible d'une forme quelconque de cyberattaque.

Gestion des risques

78 %

des sociétés canadiennes ont indiqué qu'elles prennent des mesures pour atténuer les risques liés à la cybersécurité, comme la mise en place de processus, de procédures et de systèmes.

Protection des renseignements personnels

50 %

des sociétés canadiennes ont mentionné des problèmes particuliers liés à la conformité aux lois sur la protection des renseignements personnels et ont fait part de mesures prises à cette fin.

Le contexte de la cybersécurité et de la protection des renseignements personnels

> “Plusieurs atteintes à la protection des données ont été grandement médiatisées en montrant que les cyberattaques peuvent être très dommageables et en servant de catalyseur de changement afin de pousser les organisations à communiquer de l’information sur les risques liés à la cybersécurité.
>
> **Yogen Appalraju**
> Responsable du groupe Cybersécurité, EY Canada

L’étude intitulée *2019 EY CEO Imperative Study* (en anglais) a révélé que les investisseurs et les administrateurs s’attendent à ce que les chefs de la direction relèvent un vaste éventail de défis mondiaux, et les défis associés à la cybersécurité, tant à l’échelle de l’entreprise qu’à l’échelle nationale, sont en tête de liste.

Dans l’édition 2020 de son rapport intitulé *The Global Risks Report* (en anglais), le Forum économique mondial a défini quels étaient les trois plus grands risques d’ordre technologique :

1. les cyberattaques;
2. la fraude et le vol liés aux données;
3. la perturbation d’infrastructures d’information essentielles.

Le contexte de la réglementation en matière de protection des renseignements personnels évolue, lui aussi. L’application du Règlement général sur la protection des données (RGPD) de l’Union européenne (UE) et de la California Consumer Privacy Act (CCPA) en est peut-être l’exemple le plus probant, mais la législation canadienne ne fait pas exception. Le Commissariat à la protection de la vie privée (CPVP) a entrepris un processus et une série de consultations publiques en vue de mettre à jour la réglementation canadienne, notamment la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

- À l’heure actuelle, toutes les entreprises canadiennes doivent signaler au CPVP les atteintes à la sécurité des données si elles présentent un « risque réel de préjudice grave » à l’endroit des personnes touchées.
- Dans un avenir rapproché, des modifications qui seront apportées à la législation fédérale sur la protection de la vie privée pour soutenir la Charte canadienne du numérique donneront plus de pouvoirs aux particuliers, et les autorités harmoniseront les dispositions législatives canadiennes avec les normes internationales en matière de protection de la vie privée.

Directives canadiennes et américaines en matière de communication d’informations sur les questions de cybersécurité et de protection des renseignements personnels

Les Autorités canadiennes en valeurs mobilières (ACVM) et d’autres institutions ont envoyé un message très clair : les risques liés à la cybersécurité doivent être pris très au sérieux. De plus, les sociétés ouvertes doivent communiquer aux marchés une quantité suffisante d’informations actuelles au sujet des mesures qu’elles prennent pour répondre aux cyberrisques, afin de permettre aux investisseurs de prendre des décisions éclairées.

Les ACVM ont publié les avis suivants au sujet de la cybersécurité. Ces avis soulignent la pertinence de la communication d’informations sur la cybersécurité ainsi que les attentes des ACVM à l’égard des sociétés ouvertes canadiennes, à savoir que celles-ci doivent répondre avec exactitude et sans détour aux défis que posent la cybersécurité et la protection des renseignements personnels et communiquer la nature de ceux-ci aux investisseurs.

Figure 1 : Chronologie des avis des ACVM sur la cybersécurité

1. **Avis 11-326 du personnel des ACVM**
   Septembre 2013
   On explique pourquoi il est important pour les émetteurs, les personnes inscrites et les entités réglementées de définir des mesures en matière de cybersécurité pour leurs systèmes de contrôle interne.

2. **Avis 11-332 du personnel des ACVM**
   Septembre 2016
   Les ACVM déclarent que la cybersécurité est une priorité et rappellent aux organisations qu'il faut prêter attention aux cybermenaces étant donné l'évolution de ce phénomène.

3. **Avis 51-347 du personnel des ACVM**
   Janvier 2017
   Les ACVM présentent les résultats de leur revue de l'information sur les risques liés à la cybersécurité et les cyberattaques fournie par les entreprises constituant l'indice composé S&P/TSX.

4. **Avis 33-321 du personnel des ACVM**
   Octobre 2017
   On présente les résultats d'un sondage mené par les ACVM sur les pratiques en matière de cybersécurité et de médias sociaux.

5. **Avis 11-336 du personnel des ACVM**
   Avril 2017
   On présente de l'information sur les discussions tenues lors d'une table ronde pour débattre des questions de cybersécurité et des possibilités d'améliorer la collaboration, la communication et la coordination en cas de cyberincident de grande envergure.

6. **Avis 11-338 du personnel des ACVM**
   Octobre 2018
   Cet avis contient de l'information sur les procédures à mettre en œuvre en cas de perturbation du marché à la suite d'un cyberincident.

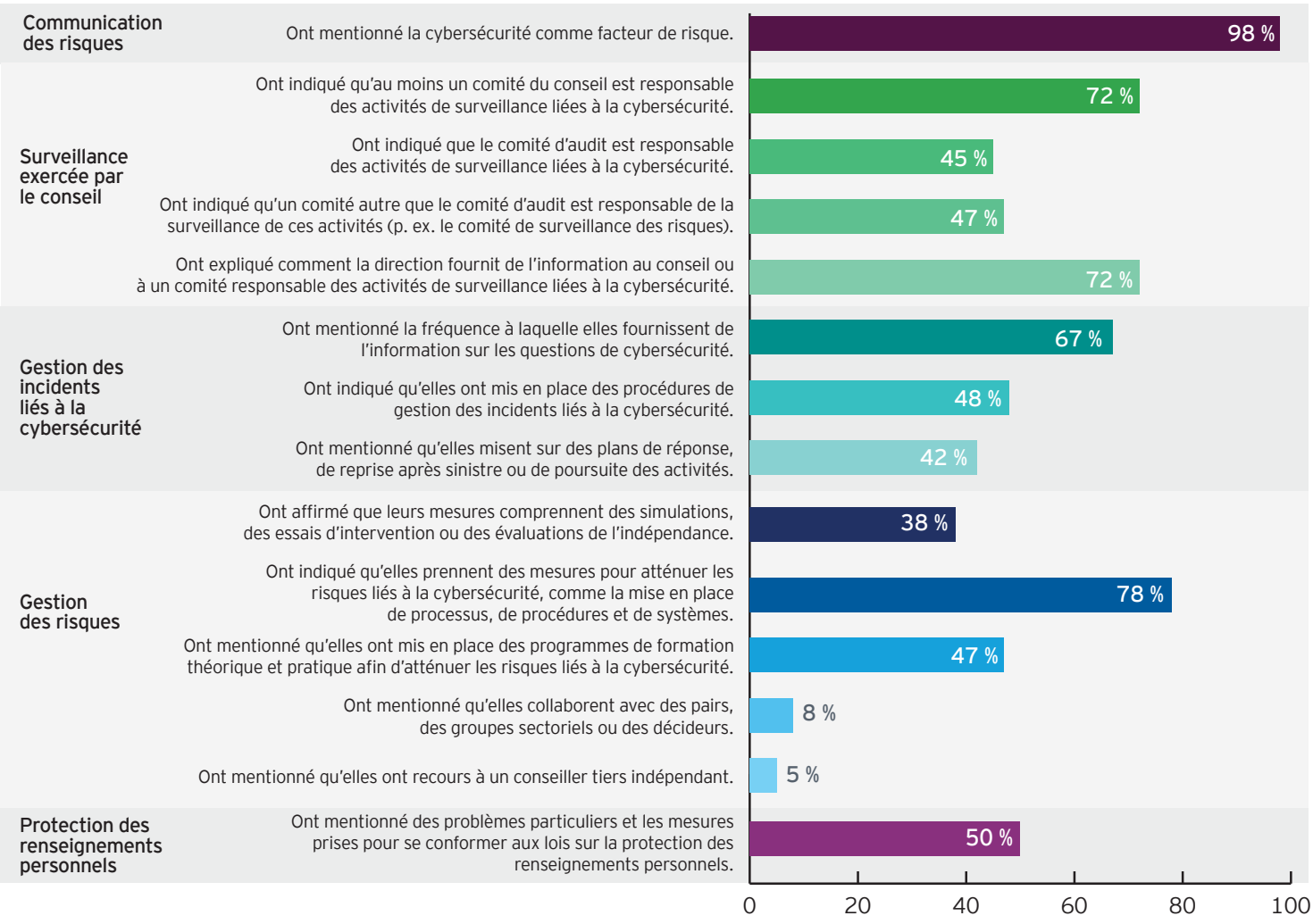
Ces avis aident les organisations à comprendre la pertinence de la communication d'informations relatives à la cybersécurité et des informations fournies à cet égard, et indiquent les mesures que les ACVM ont prises ou prendront pour relever les défis que posent les communications numériques.

La Securities and Exchange Commission (SEC) des États-Unis a publié en 2018 des directives clarifiant l'obligation qu'ont les sociétés ouvertes de fournir de l'information sur les risques liés à la cybersécurité, les atteintes majeures à la sécurité et leur incidence sur leur entreprise, leurs finances et leurs activités si elles négocient des actions aux États-Unis. Ces directives ont pour objectif de permettre aux investisseurs de prendre des décisions d'investissement éclairées, fondées sur la connaissance des risques.

Constatations

EY et CPA Canada ont analysé l'information sur la cybersécurité et sur la protection des renseignements personnels fournie dans des documents publics publiés au 31 décembre 2018 par les 60 sociétés les plus importantes (par capitalisation boursière) inscrites à la Bourse de Toronto. Ces sociétés représentent 70 % de la capitalisation boursière de la Bourse de Toronto.

Figure 2 : Constatations sur les informations relatives à la cybersécurité publiées par des sociétés ouvertes canadiennes



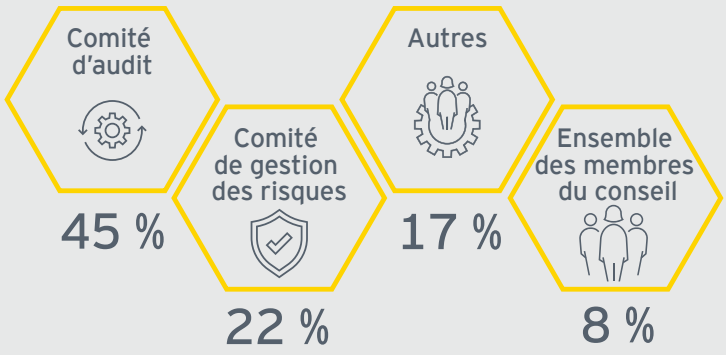
La communication d'informations sur les risques

Après analyse des résultats, nous avons constaté que la quasi-totalité des organisations canadiennes, soit 98 % d'entre elles, réalisent la pertinence des risques liés à la cybersécurité. La seule organisation analysée qui n'a pas inclus ces risques dans la section de ses documents réservée à la communication d'informations sur les risques s'est concentrée sur les risques qui peuvent avoir une incidence sur les actifs corporels.

La surveillance exercée par le conseil

Environ la moitié des organisations analysées, soit 52 %, ont attribué la responsabilité de surveiller les questions de cybersécurité à un seul comité, alors que 20 % d'entre elles l'ont attribuée à plus d'un comité, pour un total de 72 %. La figure 3 présente les comités auxquels cette responsabilité a été attribuée par les organisations analysées.

Figure 3 : Conseils qui surveillent la cybersécurité



Quarante-cinq pour cent des sociétés canadiennes confient la surveillance des questions de cybersécurité au comité d'audit, et 47 % d'entre elles, à un comité autre que le comité d'audit.

Soixante-douze pour cent des organisations canadiennes analysées communiquent les questions de cybersécurité au conseil d'administration. Soixante-sept pour cent des organisations analysées indiquent à quelle fréquence ces questions sont communiquées, comme le montre la figure 4.

Figure 4 : Fréquence à laquelle les questions de cybersécurité sont communiquées

2 %	15 %	28 %	17 %	3 %	3 %
Annuelle	Semestrielle	Trimestrielle	Tous les 5 à 8 mois	Mensuelle	Non précisée

“

Établir un plan de réponse aux situations imprévues et le tester périodiquement pour en vérifier l’efficacité est l’une des meilleures pratiques pour répondre à un incident.

Carlos Chalico
Chef d’équipe senior, Cybersécurité,
EY Canada

La gestion des incidents liés à la cybersécurité

Un peu moins de la moitié des organisations canadiennes, soit 48 %, ont affirmé avoir mis en place des procédures de gestion des incidents liés à la cybersécurité afin de réagir aux situations imprévues qui ont une incidence directe sur leurs activités de traitement électronique des données.

Ces incidents peuvent être des problèmes mineurs comme le mauvais fonctionnement d’un outil faisant appel aux technologies de l’information, ou encore des problèmes complexes comme une attaque par déni de service distribué ou une atteinte à la vie privée.

L’étude a révélé que 42 % des organisations misent sur des plans de réponse, de reprise après sinistre ou de poursuite des activités; elles ont donc mis en place des mesures pour répondre aux éventualités touchant leurs activités qui vont plus loin que leur simple capacité de traitement électronique des données.

Plus du tiers des organisations, soit 38 %, ont indiqué qu’elles misent sur des simulations, des essais d’intervention ou des évaluations de l’indépendance pour répondre aux situations imprévues.

La gestion des risques

La majeure partie des organisations analysées, soit 78 %, ont mentionné les efforts qu’elles font pour atténuer les risques liés à la cybersécurité. Le recours à des processus et des procédures spécialisés et la mise en œuvre de systèmes de gestion figurent parmi les principaux éléments mis en place pour relever ces défis. Parmi les cadres utilisés pour appuyer leur stratégie de cybersécurité, les organisations ont mentionné les normes ISO 27000[1], le cadre du NIST[2] et la norme PCI-DSS[3].

La mise en place de programmes de formation théorique et pratique afin d’atténuer les risques liés à la cybersécurité est une mesure qui a été mentionnée par 47 % des organisations analysées. À cette fin, la tenue de séances de sensibilisation à la cybersécurité et à la protection des renseignements personnels est ce que les organisations font le plus fréquemment.

Seulement 8 % des organisations ont indiqué qu’elles participent à des initiatives de collaboration afin d’échanger des idées avec leurs pairs, avec des groupes sectoriels et avec des décideurs, et de trouver les meilleures pratiques pour répondre aux défis que pose la cybersécurité. Parallèlement, 5 % des organisations font appel à un conseiller externe en cybersécurité.

1 Normes de la série 27000 publiées par l’Organisation internationale de normalisation.
2 National Institute of Standards and Technology.
3 Norme de sécurité sur les données de l’industrie des cartes de paiement.

Photo : Geran De Klerk sur Unsplash

La protection des renseignements personnels

Au moment où le Canada est en train de modifier la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) pour obliger les entreprises canadiennes à aviser les consommateurs des violations de données qui représentent un risque réel de préjudice grave pour les personnes touchées, 50 % des organisations canadiennes analysées ont dit souhaiter se conformer à la réglementation sur la protection des renseignements personnels, dont la LPRPDE et le RGPD de l'UE, entre autres.

Un cinquième des organisations analysées, soit 20 %, ont mentionné qu'elles avaient été la cible d'une forme quelconque de cyberattaque. Ces organisations font partie de secteurs divers, dont les services financiers, le commerce de détail, les produits de consommation, le secteur minier, les technologies, les télécommunications et les services. Neuf organisations ayant subi une cyberattaque ont qualifié celle-ci de peu importante, tandis que trois l'ont qualifiée d'importante.

Vos clients peuvent courir le plus grand risque durant une cyberattaque.

Dans le cas d'une cyberattaque importante, ce sont les clients de l'organisation qui ont été les plus touchés.

Dans un certain nombre de cas, ce sont les systèmes et programmes de fidélisation qui étaient ciblés.

À la suite de certaines de ces cyberattaques, des recours collectifs ont été intentés.

Conclusion

Ce rapport a pour objet de stimuler la discussion sur la communication d'informations relatives à la cybersécurité en jetant une lumière nouvelle sur les pratiques actuelles de communication de l'information et en présentant des points de vue recueillis par EY dans ses contacts avec les investisseurs et les conseils d'administration.

Les cyberattaques représentent une menace réelle que les sociétés doivent considérer comme un élément important de leur programme de gestion des risques d'entreprise. La publication d'informations donne aux sociétés l'occasion d'indiquer comment elles montrent l'exemple en relevant les défis que posent la cybersécurité et la protection des renseignements personnels. En faisant preuve de transparence, elles montrent non seulement qu'elles agissent avec prudence et diligence, mais aussi qu'elles souhaitent entretenir un dialogue avec leurs parties prenantes.

> “La cybersécurité, les pertes d'emploi attribuables aux progrès technologiques et l'inégalité des revenus constituent les trois principaux défis des chefs de direction à l'échelle mondiale. Ainsi la cybersécurité et la protection des renseignements personnels figurent parmi les huit priorités des conseils d'administration en 2020.

Michael Massoud
Directeur de projets, Recherche, orientation et soutien, CPA Canada

Questions que la direction et le conseil d'administration devraient prendre en considération

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.

Comprendre le niveau de risque du secteur et l'exposition au risque des parties prenantes

- Avons-nous décrit dans un document le cyberespace dans lequel nos partenaires commerciaux, nous-mêmes et d'autres parties prenantes exerçons nos activités et en avons-nous une compréhension approfondie?
- Avons-nous pris des mesures pour comprendre les préoccupations que les investisseurs peuvent avoir au sujet de notre exposition aux risques liés à la cybersécurité et la façon dont nous devrions aborder ces préoccupations dans l'information que nous communiquons?
- 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?
- Avons-nous évalué l'information sur les risques liés à la cybersécurité communiquée par d'autres sociétés de notre secteur ou par des sociétés d'autres secteurs dans des circonstances semblables?

Atténuer les risques par la formation du personnel et la structure de gouvernance

- 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?

Évaluer et consigner les politiques et procédures internes

- Avons-nous évalué si l'information que nous communiquons sur les risques liés à la cybersécurité, compte tenu des considérations énoncées dans les Avis du personnel des ACVM, est adéquate dans l'ensemble?
- 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 pratiques en matière de communication de l'information?
- Avons-nous établi des procédures internes pour évaluer l'importance relative des atteintes à la cybersécurité ou d'autres incidents?
- La conception de nos contrôles et de nos procédures permet-elle de nous 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?
- 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?

Ressources connexes

Pour en savoir davantage, vous pouvez consulter les ressources suivantes.

Ressources de CPA Canada

Cybersécurité : Gestion des risques et réévaluation des pratiques de communication de l'information

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

La cybersécurité vous intéresse?

Tendances en matière d'information et de pratiques liées à la cybersécurité

Ressources d'EY

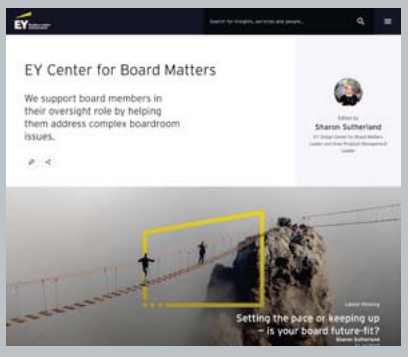
EY CEO Imperative Study (en anglais)

Sondage mondial sur la sécurité de l'information (en anglais)

Eight priorities for boards in 2020 (en anglais)

What companies are sharing about cybersecurity risk and oversight (en anglais)

EY Center for Board Matters (en anglais)



IAPP-EY Annual Privacy Governance Report (en anglais)

Personnes-ressources

Michael Massoud

CPA, CA, CPA (Illinois, É.-U.)
Directeur de projets, Recherche, orientation et soutien
CPA Canada

mmassoud@cpacanada.ca

Yogen Appalraju

CPA, CA, CISA
Responsable du groupe Cybersécurité,
EY Canada

yogen.appalraju@ca.ey.com

Carlos Chalico

CISA, CISSP, CISM, CGEIT, CRISC,
ISO 27001 LA, diplôme postbaccalauréat en comptabilité
Chef d'équipe senior, Cybersécurité,
EY Canada

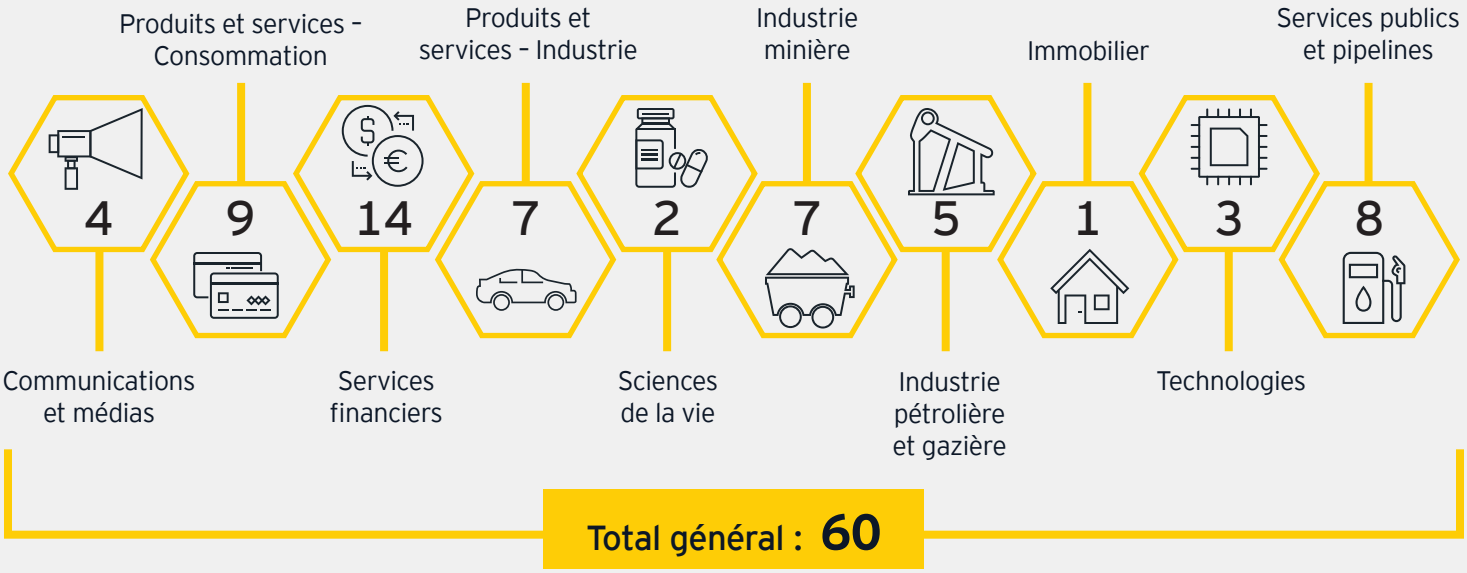
carlos.perez.chalico@ca.ey.com

Annexe
Étendue et méthode

Les constatations publiées dans le présent rapport reposent sur un examen des rapports de 2018 déposés auprès des autorités en valeurs mobilières par les 60 sociétés à grande capitalisation les plus importantes inscrites à la Bourse de Toronto et publiés dans le Système électronique de données, d'analyse et de recherche (SEDAR). L'examen a porté sur les notices annuelles, les rapports de gestion, les états financiers et les circulaires de sollicitation de procurations.

Sélection des sociétés

Les 60 sociétés canadiennes ayant fait l'objet de l'examen représentent 70 % de la capitalisation boursière[4] de l'indice composé S&P/TSX (Bourse de Toronto) et de l'indice composé S&P/TSX de croissance (Bourse de croissance TSX) pour 10 grands secteurs. Les sociétés ont été sélectionnées de façon à assurer une représentation de tous les secteurs. Le tableau ci-dessous montre le nombre de sociétés canadiennes examinées, par secteur.



4 Le pourcentage relatif à la capitalisation boursière est calculé en date du 31 décembre 2018.

Analyses

La liste de mots clés suivante a été dressée à la lumière des commentaires des répondants au sondage afin de déterminer si leurs commentaires devaient être pris en compte aux fins du présent rapport.

Les commentaires contenant ces mots clés ont servi à dégager les tendances qui sont soulignées dans le présent document. Les mots clés retenus aux fins de cet exercice sont présentés dans le tableau suivant :

attaque	ensemble de données	mots de passe
attaqué	ensemble des données	pénétration
attaquant	plan antisinistre; plan anti-sinistre	renseignements personnels
attaquants	plan de reprise après sinistre	Loi sur la protection des renseignements personnels et les documents électroniques
attaques	PA	hameçonnage
PPAS	chiffrement des données	LPRPDE
robot	RGPD	protection des renseignements personnels
plan de poursuite des activités	Règlement général sur la protection des données	renseignements protégés
renseignements confidentiels	pirates informatiques	rançongiciel
cyber	piratage informatique	résilience
assurance contre les cyberrisques	incident	accès restreint
cyber sécurité	plan d'intervention en cas d'incident	racine
cybersécurité	sécurité de l'information	renseignements sensibles
cyber-sécurité	technologie de l'information	superviseur
information relative à la cybersécurité	intrusion	accès non autorisé
atteinte à la sécurité des données	PII	virus
atteintes à la sécurité des données	accès limité	les virus; des virus
fuite de données	logiciels malveillants	vulnérabilités
confidentialité des données	maliciel	vulnérabilité
gestion des risques liés aux données	mot de passe	vers

EY | Certification | Fiscalité | Services transactionnels | Services consultatifs

À propos d'EY
EY est un chef de file mondial des services de certification, services de fiscalité, services transactionnels et services consultatifs. Les points de vue et les services de qualité que nous offrons contribuent à renforcer la confiance à l'égard des marchés financiers et des diverses économies du monde. Nous formons des leaders exceptionnels, qui unissent leurs forces pour assurer le respect de nos engagements envers toutes nos parties prenantes. Ce faisant, nous jouons un rôle crucial en travaillant ensemble à bâtir un monde meilleur pour nos gens, nos clients et nos collectivités.

EY désigne l'organisation mondiale des sociétés membres d'Ernst & Young Global Limited, lesquelles sont toutes des entités juridiques distinctes, et peut désigner une ou plusieurs de ces sociétés membres. Ernst & Young Global Limited, société à responsabilité limitée par garanties du Royaume-Uni, ne fournit aucun service aux clients.

3400510
DE 00

ey.com/ca/fr

À propos de CPA Canada
CPA Canada, l'une des organisations comptables nationales les plus importantes au monde, est une voix respectée dans les domaines des affaires et de l'enseignement de même que dans la fonction publique et le secteur des organismes sans but lucratif.

CPA Canada est une organisation progressiste et avant-gardiste dont les membres conjuguent valeurs communes, compétences diversifiées et talents exceptionnels dans leur domaine. Au pays, CPA Canada collabore avec les ordres provinciaux et territoriaux qui encadrent la profession de CPA. À l'étranger, elle travaille conjointement avec l'International Federation of Accountants et la Global Accounting Alliance pour renforcer la profession comptable partout dans le monde. CPA Canada est l'une des plus importantes organisations comptables au monde, ce qui lui donne une voix forte et influente, dont elle se sert pour agir dans l'intérêt public.

cpacanada.ca