les.cyberattaques

Elles devraient vous empêcher de fermer l'oeil

Sénat | Senate
Canada

RAPPORT DU COMITÉ SÉNATORIAL PERMANENT DES BANQUES ET DU COMMERCE

L'honorable Doug Black, c.r., président
L'honorable Carolyn Stewart Olsen, vice-présidente

OCTOBRE 2018

SÉNAT | SENATE
CANADA

Renseignements :
Par courriel : *BANC@sen.parl.gc.ca*
Par la poste : Comité sénatorial permanent des banques et du commerce
Sénat, Ottawa (Ontario), Canada, K1A 0A4
Le rapport peut être téléchargé à l'adresse suivante : *www.senate-senat.ca/*
Le Sénat est présent sur Twitter : @SenateCA,
suivez le comité à l'aide du mot-clic #BANC

This report is also available in English.

TABLE DES MATIÈRES

MEMBRES DU COMITÉ

L'honorable sénateur Doug Black, c.r., *président*
L'honorable sénatrice Carolyn Stewart Olsen, *vice-présidente*

Les honorables sénateurs

Jean-Guy Dagenais
Joseph A. Day
Colin Deacon
Pierrette Ringuette
Scott Tannas
David Tkachuk
Pamela Wallin
Howard Wetston

Membres d'office du comité :

Les honorables sénateurs Peter Harder, C.P., Diane Bellemare, Grant Mitchell, Larry W. Smith, Yonah Martin, Joseph A. Day, Terry M. Mercer, Yuen Pau Woo et Raymonde Saint-Germain.

Autres sénateurs ayant participé à l'étude :

Les honorables sénateurs Pierre-Hugues Boisvenu, Larry W. Campbell, Claude Carignan, C.P., Tobias Enverga, Jr., Stephen Greene, Michael L. MacDonald, Ghislain Maltais, Elizabeth Marshall, Sabi Marwah, Paul J. Massicotte, Lucie Moncion et Betty Unger.

Service d'information et de recherche parlementaires, Bibliothèque du Parlement :

Adriane Yong, analyste
Brett Stuckey, analyste

Direction des comités du Sénat :

Lynn Gordon, greffière du comité
Kalina Waltos, adjointe administrative

Direction des communications du Sénat :

Stav Nitka, agent de communications
Marcy Galipeau, agente de communications

ORDRE DE RENVOI

Extrait des *Journaux du Sénat* du mardi 17 octobre 2017 :

L'honorable sénateur Day propose, appuyé par l'honorable sénateur Eggleton, C.P.,

Que le Comité sénatorial permanent des banques et du commerce soit autorisé à étudier, pour en faire rapport, les questions et préoccupations relatives à la cybersécurité et à la cyberfraude, y compris :

- les cybermenaces pesant sur le secteur financier et commercial au Canada;
- le vol d'identité, l'atteinte à la vie privée et les autres activités frauduleuses ciblant les consommateurs canadiens et les petites entreprises;
- l'état actuel des technologies de cybersécurité;
- les mesures et les règlements liés à la cybersécurité au Canada et à l'étranger.

Que le comité présente son rapport final au plus tard le vendredi 29 juin 2018 et qu'il conserve tous les pouvoirs nécessaires pour diffuser ses conclusions dans les 180 jours suivant le dépôt du rapport final.

La motion, mise aux voix, est adoptée.

La greffière du Sénat

Nicole Proulx

Extrait des *Journaux du Sénat* du mardi 5 juin 2018 :

L'honorable sénateur Black *(Alberta)* propose, appuyé par l'honorable sénatrice McPhedran,

Que, nonobstant l'ordre du Sénat adopté le 17 octobre 2017, la date du rapport final du Comité sénatorial permanent des banques et du commerce concernant son étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude soit reportée du 29 juin 2018 au 30 novembre 2018.

La motion, mise aux voix, est adoptée.

Le greffier du Sénat

Richard Denis

LISTE DES RECOMMANDATIONS

Le comité recommande que :

1. Tous les ordres de gouvernement mettent l'accent sur l'éducation à la cybersécurité dans leurs stratégies de cybersécurité. Pour ce faire, le gouvernement fédéral devrait soutenir et financer :

   Des programmes de formation aux techniques de cybersécurité, en collaboration avec les provinces, les territoires et les municipalités, pour aider les entreprises à répondre à leurs besoins en matière de cybersécurité;

   Trois centres nationaux d'excellence en recherche sur la cybersécurité, afin de promouvoir la recherche fondamentale en science de la cybersécurité dans les universités et d'encourager les Canadiens à poursuivre des études et à faire carrière dans des domaines relatifs à la cybersécurité, ce qui pourrait permettre de doubler le nombre de diplômés possédant une expertise en la matière dans les quatre prochaines années;

   Un programme national de cyberlittératie, dirigé par le Centre canadien pour la cybersécurité, qui viserait à éduquer les consommateurs et les entreprises sur la façon d'adopter des comportements cyberrésilients. Ce programme devrait favoriser la sensibilisation à l'importance de la cybersécurité dans les écoles de premier et de deuxième cycles du secondaire et encourager la poursuite des études en sciences, en technologies, en ingénierie et en mathématiques.

2. Le gouvernement fédéral élabore des normes pour protéger les consommateurs, les entreprises et les gouvernements contre les menaces liées aux appareils qui pénètrent dans l'univers de l'Internet.

3. Le gouvernement fédéral définisse un cadre national pour l'échange rapide et souple d'information sur la cybersécurité et procède aux ajustements législatifs qui seraient requis à la Loi sur la protection des renseignements personnels et à la Loi sur la protection des renseignements personnels et les documents électroniques afin de permettre l'échange d'information sur les cybermenaces entre des entreprises privées et entre le secteur privé, le gouvernement et les organisations internationales pertinentes.

4. Le gouvernement fédéral repère les éventuelles lacunes pouvant nuire à l'échange d'information et qu'il détermine la façon dont les organismes d'application de la loi peuvent être dotés des outils nécessaires au partage actif et rapide d'information et collaborer avec les autres administrations pour poursuivre les cybercriminels.

5. Le gouvernement fédéral élabore un ensemble cohérent de normes de haut niveau en matière de cybersécurité qui seraient harmonisées avec les normes internationales les plus élevées et qui s'appliqueraient à toutes les entités participant aux secteurs d'infrastructures essentielles.

6. Le gouvernement fédéral offre des incitatifs aux entreprises, en particulier à celles œuvrant dans les secteurs des infrastructures essentielles, pour qu'elles puissent améliorer leurs pratiques en matière de cybersécurité, notamment en leur accordant des déductions pour amortissement accéléré pour les investissements dans la cybersécurité au titre de la *Loi de l'impôt sur le revenu*.

7. Le gouvernement fédéral modernise les lois canadiennes sur la protection des renseignements personnels afin de tenir compte des préoccupations émergentes en matière de cybersécurité et des normes internationales. Il devrait fournir au Commissariat à la protection de la vie privée de nouvelles ressources pour lui permettre de s'acquitter de son mandat, et conférer au commissaire le pouvoir de rendre des ordonnances et d'imposer des amendes aux entreprises qui ne prennent pas les mesures adéquates pour protéger les renseignements de leurs clients.

8. Le gouvernement fédéral crée un nouveau ministère fédéral de la cybersécurité, qui serait responsable de la politique en matière de cybersécurité, dont la stratégie nationale en matière de cybersécurité, et superviserait le nouveau Centre canadien pour la cybersécurité et l'Unité nationale de coordination de la lutte contre la cybercriminalité.

   D'ici à ce qu'un tel ministère soit créé, la personne désignée comme étant le chef de file du gouvernement fédéral en cybersécurité devrait relever directement du premier ministre sur les questions en la matière.

   Enfin, le premier ministre devrait déposer chaque année devant le Parlement un rapport sur les questions relatives à la stratégie de cybersécurité du Canada.

9. Le gouvernement fédéral crée un groupe fédéral d'experts sur la cybersécurité chargé de formuler des recommandations pour la stratégie nationale de cybersécurité qui feraient du Canada un chef de file mondial en cybersécurité.

10. Le gouvernement fédéral enjoigne à ses ministères et à ses organismes de déclarer les atteintes à la vie privée au Commissariat à la protection de la vie privée;

    Le gouvernement fédéral continue de mettre en œuvre des pratiques exemplaires à l'intention de la fonction publique fédérale pour garantir l'utilisation de dispositifs sécurisés empêchant la divulgation de renseignements de nature délicate.

INTRODUCTION

Les cyberattaques font les manchettes chaque semaine, sinon chaque jour. Des entreprises actives dans le monde entier sont réticentes à révéler – elles prennent parfois des mois ou des années à le faire – qu'elles ont fait l'objet d'une cyberattaque, et que les renseignements personnels que des Canadiens leur ont confiés peuvent être entre les mains de criminels.

> ***[…] sur une période de 25 à 30 ans, nous avons transféré presque tout ce qui est précieux pour nous dans l'Ouest de l'analogue - livres et documents – au numérique, puis nous avons relié tout ça par un protocole Internet – TCP/IP - qui n'avait jamais été conçu en fonction de la sécurité. Nous avons fait cela sans calculer correctement le risque d'une telle démarche si des terroristes, des escrocs, des espions et des États-nations exploitaient ces renseignements maintenant stockés sous forme numérique et reliés par Internet.***
>
> *John P. Carlin, président, Morrison & Foerster s.r.l., 22 mars 2018.*

Lorsqu'il a lancé une étude sur la cybersécurité, le Comité sénatorial permanent des banques et du commerce (le comité) avait orienté celle-ci au départ vers les cyberattaques qui ont compromis les données financières des Canadiens. Cependant, le comité est devenu de plus en plus préoccupé par les cyberrisques qui évoluent sans cesse et qui menacent la société canadienne tout entière, en particulier le secteur des infrastructures essentielles.

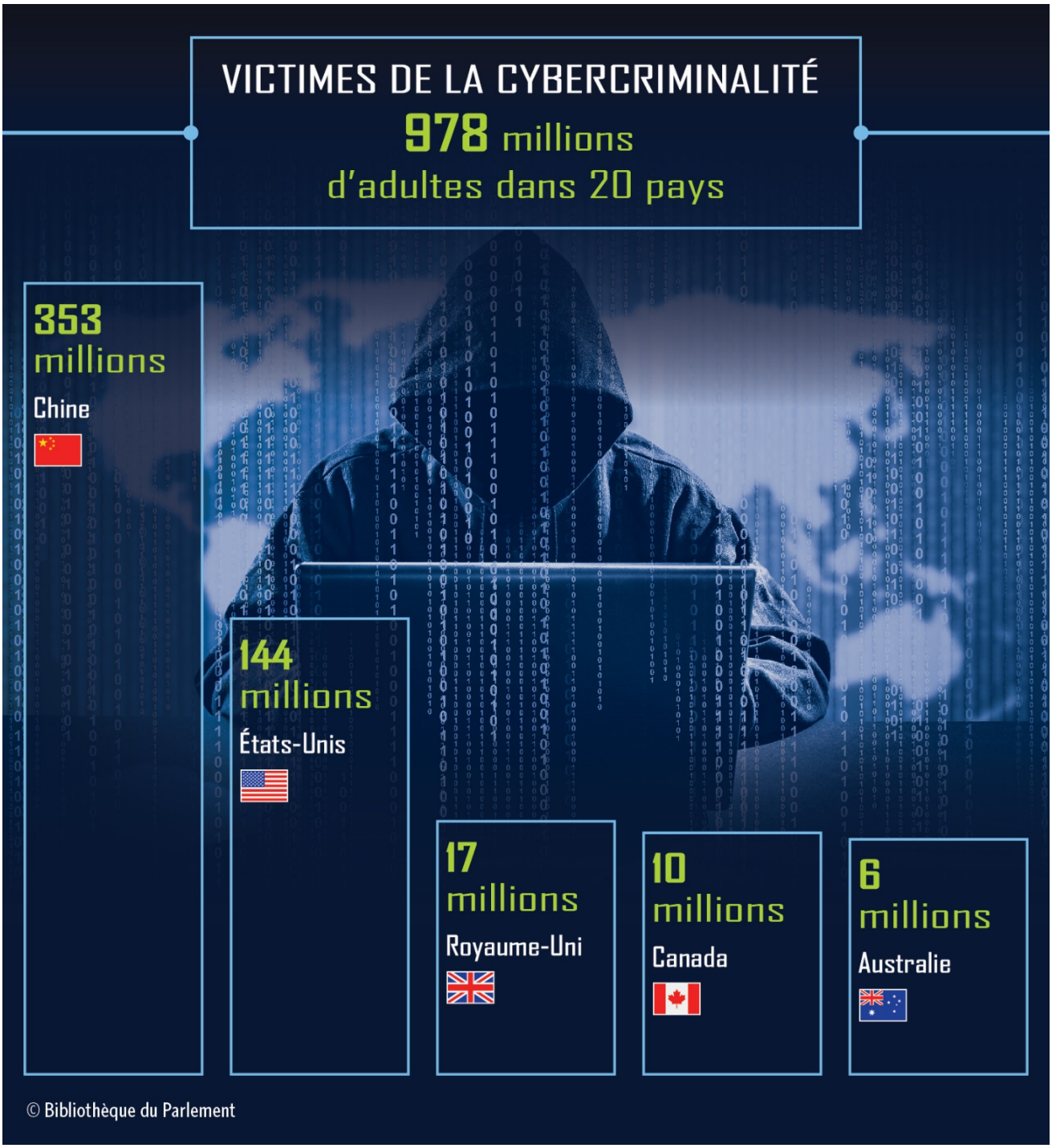
En 2017, 19 700 Canadiens se sont fait usurper leurs données financières personnelles lors d'une atteinte à la cybersécurité d'Equifax, une entreprise qui recueille des données de nature délicate d'antécédents de crédit et offre même des services de lutte contre le vol d'identité. Equifax a admis que des pirates informatiques avaient volé les renseignements personnels de 145,5 millions de consommateurs, pour la plupart des Américains. Un an plus tard, des pirates ont réussi à voler de l'information financière personnelle sur 90 000 clients de la Banque de Montréal et de la Financière Simplii (CIBC) et ont menacé de la rendre publique.

Des progrès ont été accomplis au niveau fédéral depuis un an, mais le gouvernement fédéral et les Canadiens doivent en faire davantage pour se protéger. L'heure est à la prise de mesures appropriées dès maintenant : sinon, nous serons tous des victimes.

Figure 1 : Nombre de Canadiens touchés par des atteintes à la protection des renseignements personnels survenues récemment

Source : Données compilées par les auteurs à partir de sources diverses

Figure 2 : Nombre de victimes de la cybercriminalité en 2017 dans quelques pays



Source : Norton par Symantec, 2017 Norton Cyber Security Insights Report Global Results, p. 11. [EN ANGLAIS SEULEMENT]

Au fil de leurs neuf réunions, les membres du comité ont accueilli des représentants de ministères et d'organismes du gouvernement, du Commissariat à la protection de la vie privée du Canada, du milieu de la justice, des universités, du secteur financier et d'autres regroupements d'entreprises pour en apprendre davantage sur la position du Canada en matière de cybersécurité, et les mesures que le gouvernement doit prendre pour améliorer la cybersécurité au pays.

Pensez-vous que votre cybersécurité est assurée? Participez à un jeu-questionnaire; reconnaissez-vous les cyberrisques?

Les témoins ont soulevé plusieurs questions importantes.

Plusieurs témoins ont signalé la nécessité d'investir dans l'éducation à la cybersécurité pour remédier à la pénurie de professionnels de la cybersécurité et pour aider les Canadiens à être au courant des risques liés aux connexions Internet. La façon d'éduquer efficacement les Canadiens au sujet de la cybersécurité constitue le fondement de la principale recommandation de ce rapport.

Nous avons été particulièrement découragés d'apprendre qu'à part poursuivre l'entreprise qui a été piratée, les consommateurs du Canada n'ont en général que peu de recours contre le vol de leurs renseignements personnels. On a fait remarquer que :

> Lorsqu'une entreprise est piratée, la GRC procède à une enquête lui permettant de déterminer l'identité du pirate. Cependant, la perte de renseignements des consommateurs est considérée comme une violation de contrat par l'entreprise, et pas nécessairement comme un crime qui pourrait faire l'objet d'une enquête policière. Souvent, l'entreprise ne fait même pas part de la perte de l'information personnelle aux organisations d'application de la loi. Donc, lorsque des Canadiens sont avisés de la violation de données, il leur appartient de prendre des mesures pour déterminer si des cybercriminels utilisent leurs renseignements, parce qu'aucun mécanisme n'est en place pour les aider.
>
> Pour examiner la cybersécurité, il faut comprendre les lois canadiennes en matière de protection des renseignements personnels. Le Commissariat à la protection de la vie privée surveille le respect des deux lois fédérales qui portent sur ce sujet, soit la *Loi sur la protection des renseignements personnels*, qui réglemente les renseignements personnels que détiennent les ministères et les organismes fédéraux, et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui régit les renseignements personnels que recueillent beaucoup d'entreprises canadiennes auprès de leurs clients. Les particuliers peuvent communiquer avec le Commissariat à la protection de la vie privée pour porter plainte; toutefois, le commissaire à la protection de la vie privée n'a pas le pouvoir d'obliger les entreprises à respecter la LPRPDE ou de leur imposer des amendes.

Il a également été extrêmement préoccupant d'apprendre que la Gendarmerie royale du Canada (GRC) n'a peut-être pas les capacités nécessaires pour entreprendre de nouvelles enquêtes sur les cybermenaces importantes. De plus, la GRC a aussi fait observer que :

> Au Canada, les mesures permettant de déclarer la cybercriminalité sont source de confusion chez les Canadiens et font en sorte que ces derniers ne la déclarent pas aussi souvent qu'ils le devraient. Pour cette raison, la police est incapable de procéder à une analyse exhaustive de la cybercriminalité, ce qui entrave les possibilités d'action concertée, tant au Canada qu'entre les États.

Les témoins ont aussi insisté sur l'importance de protéger les systèmes canadiens et mondiaux considérés comme des infrastructures essentielles, ainsi que sur la difficulté qu'ont les entreprises sont à empêcher leurs réseaux d'être piratés. Ils ont prévenu que :

> Il existe 10 secteurs canadiens d'infrastructures essentielles, qui sont tous connectés à Internet et sont fortement interdépendants. Les représentants du secteur financier se sont dits préoccupés par les divergences entre les normes de cybersécurité de tous ces secteurs. Ils se sont également demandé s'il était souhaitable de permettre aux plus petites sociétés disposant de ressources moindres et dont les normes de cybersécurité peuvent être inférieures, en particulier les entreprises de technologie financière, d'avoir accès aux données et aux systèmes financiers du Canada.

> De façon générale, les entreprises n'investissent pas suffisamment dans la cybersécurité parce que les effets à long terme des atteintes à la sécurité sur les cours des actions ou le comportement des consommateurs sont minimes.

> On remarque une pénurie mondiale de professionnels de la cybersécurité, et les entreprises canadiennes cherchent à se tourner vers l'étranger pour trouver des spécialistes de ce domaine.

Figure 3 : Les 10 secteurs canadiens d'infrastructures essentielles

- la santé
- l'alimentation
- les finances
- l'eau
- les technologies de l'information et de la communication
- la sécurité
- l'énergie et les services publics
- le secteur manufacturier
- le gouvernement
- les transports

En ce qui concerne la stratégie nationale du Canada en matière de cybersécurité et la sécurité nationale, les témoins ont déclaré que :

> Le gouvernement fédéral a fourni un financement par l'intermédiaire du budget fédéral de 2018 pour revaloriser le cadre national de cybersécurité du Canada et

créer le Centre canadien de cybersécurité, situé au sein du Centre de la sécurité des télécommunications, et l'Unité nationale de coordination de la lutte contre la cybercriminalité, dans le cadre de la GRC. Ces deux nouvelles entités collaboreront avec le ministère de la Sécurité publique et de la Protection civile, qui demeure responsable de la coordination et des politiques nationales. Le gouvernement a également instauré une nouvelle stratégie de cybersécurité nationale en juin 2018.

On a indiqué que, dans des pays comme les États-Unis, le Royaume-Uni, l'Australie, Israël, les Pays-Bas et Singapour, la priorité est accordée à la cybersécurité en raison de son importance en ce qui touche l'économie ainsi que la recherche et le développement.

Plutôt que de se contenter de se défendre contre les cyberattaques, les gouvernements ont recours à des cyberopérations offensives qui nuisent aux pays étrangers, aux infrastructures essentielles et aux entreprises. Les cyberattaques étant considérées comme un problème d'envergure mondiale, il convient de procéder à une surveillance à l'échelle mondiale.

Les Canadiens doivent savoir que la cybersécurité est un enjeu sérieux : les gens négligent de se protéger contre les cybermenaces courantes et émergentes. Tous les Canadiens doivent pourtant répondre à l'urgence de protéger le pays, et ce, avant que les cybercriminels puissent s'infiltrer dans nos systèmes essentiels et orchestrer une catastrophe technologique pour le Canada.

SENSIBILISER LA POPULATION CANADIENNE À LA CYBERSÉCURITÉ ET À LA RÉSILIENCE

Il a été clairement établi qu'une éducation plus poussée sur la cybersécurité est requise au Canada. Selon le Bureau du surintendant des institutions financières, la « cyberrésilience » désigne la capacité d'une institution d'anticiper ou de contenir une cyberattaque, d'y résister, ou de s'en rétablir rapidement avant que celle-ci compromette ses opérations ou qu'elle nuise à ses clients. La cyberrésilience est une responsabilité commune des gouvernements, du secteur privé et des consommateurs, car tous ont un rôle à jouer afin de protéger les principaux réseaux contre les cybermenaces à long terme.

> ***Il [devrait y avoir une] prise de conscience concernant la sécurité. Il s'agit de comprendre qu'il y a un besoin en matière de sécurité, qu'il faut protéger ses renseignements personnels; une personne décide ce qu'elle partage sur Facebook, et si elle le fait, elle doit comprendre ce que cela signifie pour ses données. Ces décisions doivent être bien comprises, probablement même avant l'école secondaire.***
>
> *Institut de la cybersécurité et de la protection des renseignements personnels, Université de Waterloo, 21 mars 2018*

L'un des trois thèmes de la stratégie de cybersécurité nationale du Canada de 2018 est l'« innovation en matière de cybersécurité », qui est composée de l'appui de la recherche avancée ainsi que du perfectionnement des compétences et des connaissances associées à la sphère numérique. Les membres du comité proposent que ce thème devienne la priorité de la stratégie et suggèrent un mécanisme en trois volets pour permettre d'améliorer l'éducation à la cybersécurité et l'importance de la cyberrésilience au Canada, tout en tenant compte du besoin de soutenir et de promouvoir les technologies novatrices et les perspectives que celles-ci ouvrent : le perfectionnement des compétences, le soutien de la recherche et du développement, et la sensibilisation du grand public et des entreprises.

Premièrement, une formation axée sur les compétences en cybersécurité est nécessaire étant donné la pénurie générale de professionnels dans ce domaine. La démarche adoptée par le comité en matière de perfectionnement des compétences obligerait le gouvernement fédéral à consulter des représentants du secteur privé ainsi que des provinces et des territoires afin d'élaborer des programmes nationaux de formation professionnelle en cybersécurité pour aider les entreprises à répondre à leurs besoins à court terme à cet égard. Ces types de programmes pourraient inclure la formation des employés actuels, des programmes à l'intention des cadres qui mettent l'accent sur une évaluation des risques ou sur les moyens de conserver les services de professionnels de la cybersécurité qualifiés, et,

pour les élèves inscrits à l'école secondaire et à l'université, des postes de stagiaire dans des entreprises d'informatique ou de cybersécurité pour leur permettre de comprendre les domaines de la cybersécurité. Les entreprises canadiennes ont besoin d'aide maintenant, ce qui requiert des investissements dans la formation pour l'acquisition de compétences.

Deuxièmement, le gouvernement fédéral doit financer la recherche fondamentale en science de la cybersécurité. Des recherches scientifiques et technologiques fondamentales sont nécessaires si l'on veut répondre à des questions essentielles en matière de cybersécurité, comme ce que l'on entend par la notion de « protection des renseignements ». Une fois que ces principes seront établis, les spécialistes de la cybersécurité pourront trouver les meilleures solutions pratiques qui contribueront à améliorer les normes et les opérations de cybersécurité du Canada.

Constituer un bassin de talents du Canada passe, entre autres, par de meilleurs programmes éducatifs pour une carrière en cybersécurité, la formation du personnel actuel, des pratiques avérées de gestion du développement des carrières, ainsi qu'une pollinisation croisée créative avec des disciplines en forte demande et étroitement liées à la cybersécurité.

Association des banquiers canadiens, 26 octobre 2017

Certains pays ont déjà perfectionné la recherche et l'expertise dans le domaine de la cybersécurité. Par exemple, la National Security Agency des États-Unis a désigné certains programmes universitaires dans plusieurs universités américaines comme des centres nationaux d'excellence en cyberopérations ou en cyberdéfense, en vue de promouvoir l'enseignement supérieur et la recherche en cyberdéfense et en sécurité, et de former des professionnels en matière de cybersécurité capables de soutenir tant le secteur privé que le gouvernement.

L'Allemagne a créé l'Association Helmholtz des centres de recherche allemands, qui effectue de la recherche dans divers domaines scientifiques et technologiques. Au Centre de sécurité des TI, de confidentialité des renseignements et d'obligation de rendre des comptes, ou Centre Helmholtz (i.G.) GmbH, connu sous le nom de CISPA, inauguré en décembre 2017, plus de 500 chercheurs examineront les défis importants liés à la recherche sur la cybersécurité et sur la protection de la vie privée que pose une société numérique.

Le Canada, quant à lui, dispose du Programme des réseaux de centres d'excellence, en vertu duquel le Réseau intégré sur la cybersécurité (SERENE-RISC est financé. Cependant, afin que nous demeurions pertinents et concurrentiels face aux autres pays, le gouvernement fédéral doit créer et financer adéquatement des centres nationaux d'excellence spécialement conçus pour effectuer de la recherche fondamentale sur la cybersécurité. Il faudrait établir trois centres d'excellence : l'Institut canadien de la cybersécurité de l'Université du Nouveau-Brunswick, le Cybersecurity and Privacy Institute

de l'Université de Waterloo, et un troisième, qui serait situé dans l'Ouest du Canada. Cela encouragera d'autres universités canadiennes à mettre sur pied des programmes similaires. Ces programmes universitaires attireront des étudiants du monde entier et les aideront à acquérir les compétences et l'expertise en cybersécurité dont tant le secteur privé que le secteur public ont désespérément besoin. L'objectif consiste à accroître de 100 % le nombre de diplômés possédant un savoir-faire en matière de cybersécurité.

> ***Internet et d'autres systèmes en ligne permettent à des criminels et à d'autres acteurs de retirer les composantes d'interactions personnelles, et certaines de ces capacités de communication que, comme nous le voyons, les gens utilisent lorsqu'il y a une menace et lorsqu'il n'y en a pas.***
>
> *Gendarmerie royale du Canada, 18 octobre 2017*

Troisièmement, les membres du comité proposent que le gouvernement fédéral cherche des moyens d'éduquer efficacement la population et les entreprises à la cybersécurité et à la cyberrésilience. Les citoyens ordinaires et les petites entreprises sont les victimes d'arnaques en ligne comme des tentatives d'hameçonnage et des maliciels, et la plupart d'entre eux ne savent pas comment faire face à ces menaces, à qui s'adresser lorsque celles-ci se produisent ou comment se protéger contre d'autres attaques.

Une stratégie nationale de cyberlittératie, semblable à la stratégie de littératie financière du Canada supervisée par l'Agence de la consommation en matière financière du Canada, permettrait à tous les Canadiens de disposer de connaissances et d'outils qui leur serviront à se défendre contre les menaces actuelles et futures. Le nouveau Centre canadien pour la cybersécurité pourrait gérer cette stratégie, qui serait élaborée en collaboration avec les provinces et les territoires, ainsi qu'avec des intervenants comme des institutions financières et des entreprises en cybersécurité, qui travailleraient directement avec les Canadiens victimes d'une cyberattaque. Il devrait se concentrer sur la manière d'éduquer efficacement les Canadiens à tous les niveaux de connaissances en informatique, ainsi que sur les outils que le gouvernement fédéral pourrait fournir aux personnes et aux entreprises pour leur permettre d'assurer la sécurité de leurs ordinateurs, de leurs réseaux et de leurs systèmes.

Figure 4 : Conseils que devraient suivre les consommateurs afin de protéger leurs renseignements personnels

1. Pensez-y deux fois avant de partager des renseignements personnels en ligne ou en personne.
2. Posez des questions au sujet de la position de confidentialité de l'entreprise quant aux renseignements des clients.
3. Si vous vous inquiétez de la façon dont vos renseignements personnels sont traités, exprimez¬-vous et faites-le savoir à l'entreprise.
4. Lorsqu'une entreprise vous demande des renseignements personnels, refusez, tout simplement, et inscrivez-vous aux listes des numéros de téléphone barrés ou des personnes qui ne souhaitent pas recevoir de courrier.
5. Protégez votre numéro d'assurance sociale : il s'agit d'une information confidentielle qui ne devrait être communiquée qu'à des fins de déclaration de revenus.
6. Protégez le contenu vos appareils au moyen de mots de passe, de logiciels, d'antivirus, d'antipourriel ainsi que de pare-feu, et pensez à chiffrer vos données de nature délicate et à désactiver le Wi-Fi et votre Bluetooth lorsque vous ne les utilisez pas.
7. Protégez vos mots de passe en les rendant difficiles à deviner et utilisez des mots de passe différents pour chaque compte, chaque site Web et chaque dispositif.
8. Familiarisez-vous avec les paramètres de confidentialité des appareils, des navigateurs, des sites Web, des applications et des caméras que vous utilisez, et ajustez-les régulièrement.
9. Supprimez adéquatement les données stockées dans les appareils que vous n'utilisez plus, que vous vendez ou que vous recyclez.
10. Connaissez vos droits à la vie privée en vertu des lois fédérales et provinciales en matière de protection des renseignements personnels.

Source : Commissariat à la protection de la vie privée du Canada, Dix conseils à suivre pour protéger vos renseignements personnels

Il est important que les enfants canadiens, en raison de leur utilisation des médias sociaux et d'autres technologies numériques lorsqu'ils sont encore très jeunes, prennent conscience des risques liés à l'utilisation d'Internet bien avant d'entrer à l'université. Dans le cadre de la stratégie de cyberlittératie, il faudrait souligner la nécessité de protéger les renseignements personnels dans les écoles secondaires du premier et du deuxième cycle, et encourager les élèves à poursuivre leurs études en sciences, en technologie, en ingénierie et en mathématiques. Le gouvernement fédéral doit travailler en partenariat avec les provinces et les territoires afin que les programmes d'études scolaires reflètent ces objectifs.

S'ils réfléchissent à de telles questions dès le secondaire, les jeunes Canadiens pourront apprendre à se protéger, leur famille et eux, contre les cybermenaces, adopter d'excellentes pratiques en matière de cybersécurité et songer à faire carrière en informatique et en cybersécurité.

Le comité recommande donc que **:**

Tous les ordres de gouvernement mettent l'accent sur l'éducation à la cybersécurité dans leurs stratégies de cybersécurité. Pour ce faire, le gouvernement fédéral devrait soutenir et financer :

Des programmes de formation aux techniques de cybersécurité, en collaboration avec les provinces, les territoires et les municipalités, pour aider les entreprises à répondre à leurs besoins en matière de cybersécurité;

Trois centres nationaux d'excellence en recherche sur la cybersécurité, afin de promouvoir la recherche fondamentale en science de la cybersécurité dans les universités et d'encourager les Canadiens à poursuivre des études et à faire carrière dans des domaines relatifs à la cybersécurité, ce qui pourrait permettre de doubler le nombre de diplômés possédant une expertise en la matière dans les quatre prochaines années;

Un programme national de cyberlittératie, dirigé par le Centre canadien pour la cybersécurité, qui viserait à éduquer les consommateurs et les entreprises sur la façon d'adopter des comportements cyberrésilients. Ce programme devrait favoriser la sensibilisation à l'importance de la cybersécurité dans les écoles de premier et de deuxième cycles du

secondaire et encourager la poursuite des études en sciences, en technologies, en ingénierie et en mathématiques.

Figure 5 : Protéger ses renseignements personnels

Source : Préparé par les auteurs

AMÉLIORER LA STRATÉGIE DE CYBERSÉCURITÉ DU CANADA

En plus d'accorder la priorité à l'éducation à la cybersécurité, les témoins ont fait d'autres suggestions visant à améliorer les pratiques des Canadiens en matière de cybersécurité, entre autres sensibiliser les consommateurs aux risques associés à l'Internet des objets, aider les entreprises canadiennes à répondre à leurs besoins en matière de cybersécurité et à respecter les lois en matière de protection des renseignements personnels, et modifier le cadre national de cybersécurité.

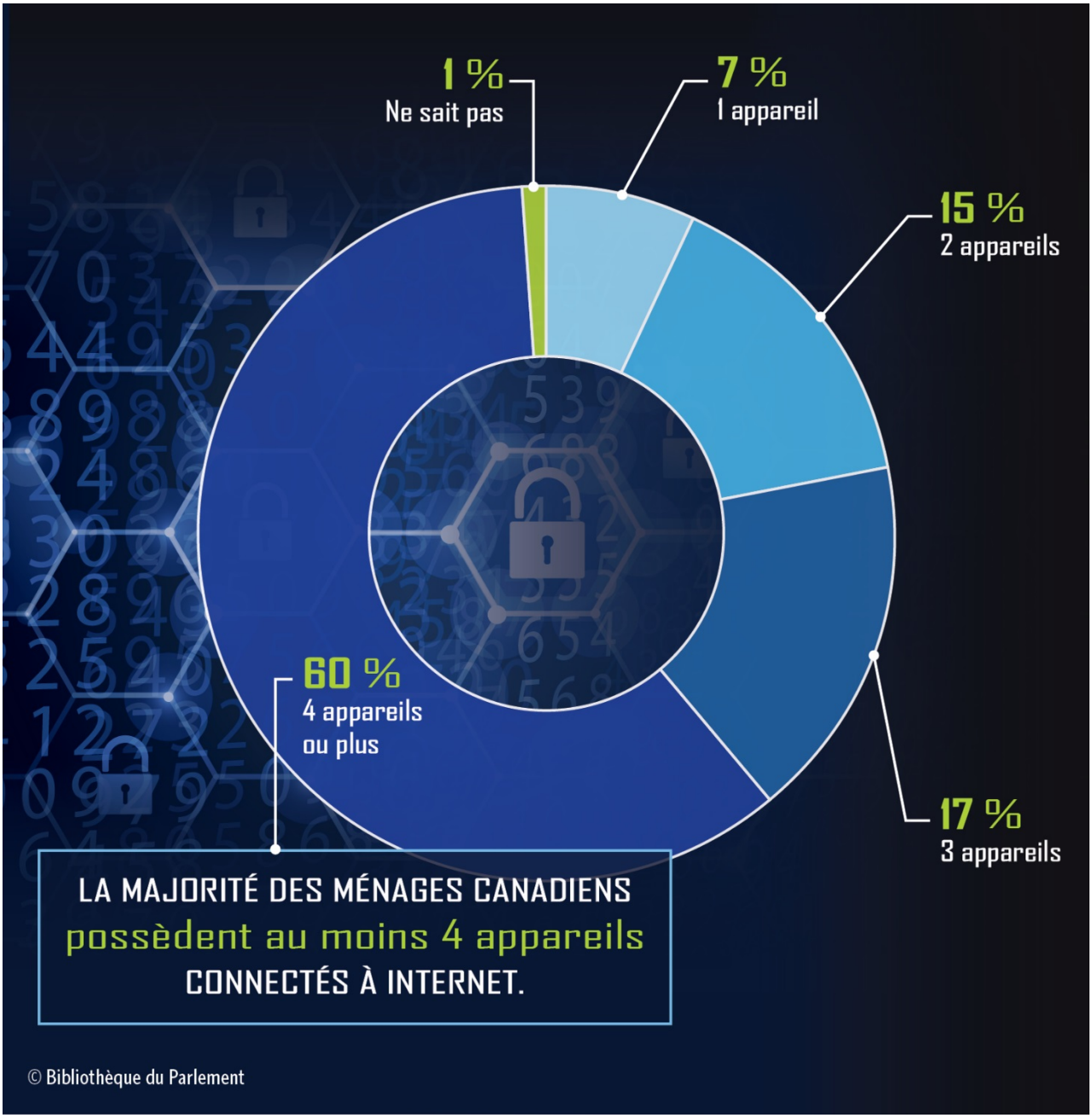
A. Sensibiliser les consommateurs aux risques présents dans l'univers de l'Internet des objets

Les témoins se sont dits préoccupés par le réseau grandissant d'appareils reliés à Internet sur le marché, mieux connus sous le nom d'Internet des objets, et par les risques que ceux-ci représentent pour les consommateurs. L'Internet des objets, c'est bien plus que des dispositifs domestiques comme des moniteurs de surveillance pour bébé, des réfrigérateurs et des thermostats. Cela comprend les capteurs installés sur les routes, les véhicules autonomes et les machines dotées de capacités d'intelligence artificielle, et c'est devenu un facteur de changement pour de nombreuses entreprises. Ce type d'appareil facilite la vie des consommateurs canadiens et la rend plus agréable. Toutefois, la commodité est synonyme de risques considérables touchant la cybersécurité, puisque, lorsque ces appareils sont conçus, la sécurité n'est pas prioritaire.

Comme on peut le voir à la figure 6, plus de la moitié des ménages canadiens possèdent au moins quatre appareils connectés à Internet, et chacun de ces appareils peut devenir une cible pour les cybercriminels.

> ***Selon moi, il faudrait probablement tenir une conversation élargie sur l'Internet des objets ou de tout, pour reprendre l'appellation qu'utilisent certaines entreprises pour parler des milliards d'appareils déployés qui n'ont pas été nécessairement conçus avec la sécurité en tête, comme la domotique, l'intelligence artificielle ou, au moins, l'apprentissage machine. Je pense que c'est là un des défis les plus importants que nous aurons à relever au cours des 10 prochaines années.***
>
> *Chambre de commerce du Canada, 1er mars 2018*

Figure 6 : Nombre d'appareils reliés à Internet dans les ménages du Canada, 2017



Source : Autorité canadienne pour les enregistrements Internet, Le dossier documentaire d'Internet 2018, p. 13

Des exemples récents montrent que les dispositifs connectés à Internet qui sont vulnérables aux cyberattaques pourraient avoir une incidence énorme sur la sécurité des consommateurs. En 2015, il a été prouvé que certains modèles de Jeep pouvaient être piratés par le biais de leur système de divertissement, ce qui risque de permettre au pirate

de prendre le contrôle des systèmes de freinage et de direction de l'automobile. Jeep a dû rappeler 1,4 million de voitures. En 2017, la Food and Drug Administration des États-Unis a quant à elle rappelé près d'un demi-million de stimulateurs cardiaques parce qu'elle craignait que ceux-ci ne soient piratés si des mises à jour appropriées n'y étaient pas effectuées.

Le gouvernement fédéral doit se pencher sur les façons dont ces appareils devraient être sécurisés avant qu'ils arrivent sur le marché. Tous les dispositifs devraient-ils être chiffrés? Faudrait-il différents niveaux d'attestation de sécurité? Comment les appareils seront-ils mis à jour? Le gouvernement devrait-il certifier les appareils dont les mesures de cybersécurité sont adéquates?

> ***Les cyberactivités parrainées par un État visent notamment à obtenir de l'information qui permettrait à des sociétés étrangères de jouir d'un avantage concurrentiel sur les entreprises canadiennes. Cela peut nuire aux négociations liées à des projets d'investissement ou d'achat entre des entreprises canadiennes et le gouvernement du Canada, puis entraîner la perte d'emplois, de revenus et de parts de marché. En définitive, le cyberespionnage a une incidence négative sur l'économie du Canada dans son ensemble***
>
> *Service canadien du renseignement de sécurité, 18 octobre 2017*

Si ces appareils doivent être déployés dans des systèmes d'infrastructures essentielles, d'autres considérations pourraient inclure la détermination du type d'essai à effectuer pour s'assurer qu'ils sont cybersécuritaires, et le fait de savoir s'ils pourraient être utilisés pour le cyberespionnage.

Ce ne sont que quelques-unes des questions que le gouvernement fédéral doit étudier pour déterminer quels types de normes il lui faudrait élaborer pour contrer les cybermenaces possibles visant les appareils des Canadiens et les infrastructures essentielles.

Par conséquent, le comité recommande que :

Le gouvernement fédéral élabore des normes pour protéger les consommateurs, les entreprises et les gouvernements contre les menaces liées aux appareils qui pénètrent dans l'univers de l'Internet.

B. Aider les entreprises canadiennes et vérifier leur conformité aux lois sur la protection des renseignements personnels

Le secteur privé joue un rôle essentiel dans le cadre de la stratégie de cybersécurité du Canada. Les entreprises fournissent des services d'infrastructures essentielles et sont donc des cibles importantes des cybercriminels nationaux et de ceux parrainés par les États. Elles recueillent de vastes quantités d'information auprès des consommateurs et doivent par conséquent protéger contre les cybermenaces à la fois leurs bases de données et tout réseau auquel elles sont reliées. Le comité s'inquiète particulièrement au sujet des petites entreprises des dix secteurs d'infrastructures essentielles au Canada. Contrairement à l'administration fédérale et aux grandes entreprises comme les banques, ces petites entreprises n'ont généralement pas les ressources nécessaires pour protéger efficacement leurs systèmes.

Remédier par l'éducation au manque de professionnels en matière de cybersécurité permettra d'assurer la cybersécurité à long terme des entreprises, mais il reste encore du travail à accomplir pour répondre aux préoccupations à court et à moyen terme du secteur privé à cet égard et pour protéger l'économie dans l'ensemble.

1. Permettre l'échange de renseignements pour le secteur privé et les gouvernements

Les cyberattaques se propagent rapidement, et les gouvernements doivent souvent échanger de l'information et des renseignements de sécurité avec d'autres pays pour les contrer. De même, en raison de l'interconnexion des réseaux mondiaux d'infrastructures essentiels, ils pourraient devoir échanger rapidement des renseignements sur les consommateurs pour réagir efficacement à une menace. Il faut que le gouvernement et le secteur privé se coordonnent pour réagir sans délai aux cyberattaques, notamment en communiquant des renseignements délicats et confidentiels. Toutefois, la communication de renseignements gouvernementaux peut s'avérer difficile, car ces renseignements peuvent être classifiés. En effet, les entreprises ne peuvent partager avec d'autres entreprises ou avec leurs clients que de l'information de nature limitée ou très générale sur certains types de cybercrimes.

> ***Les renseignements sur les menaces cybernétiques sont importants pour plusieurs raisons. L'échange de renseignements nous permet de miser sur les connaissances des autres et rend les attaques plus coûteuses. Il permet d'enrichir les renseignements sur les menaces cybernétiques consignés par les entreprises, ce qui les rend plus exploitables. Les renseignements opportuns et exploitables nous permettent de renforcer notre cyberdéfense.***
>
> *Échange canadien de menaces cybernétiques, 1er mars 2018*

Le gouvernement fédéral devrait examiner les initiatives mises sur pied par des organisations comme l'Échange canadien de menaces cybernétiques, permettant aux entreprises de partager de l'information sur les cybermenaces et les pratiques en matière de cybersécurité dans un environnement sûr avec d'autres entreprises, le gouvernement et des instituts de recherche. Ce faisant, il aurait pour mandat de concevoir un cadre national de partage de renseignements permettant de lutter contre les cybermenaces. Le cadre énoncerait pour sa part les paramètres applicables à la communication de renseignements entre des sociétés privées, le gouvernement et d'autres organisations internationales pertinentes. Il faudrait se pencher sur les dispositions législatives en matière de protection des renseignements personnels pour déterminer comment faciliter l'échange de renseignements tout en continuant de respecter les droits en matière de protection de la vie privée des Canadiens.

> ***Il apparaît clairement nécessaire d'assurer une coordination publique-privée pour réagir aux attaques contre les infrastructures essentielles, et aussi de déterminer dans le secteur public un seul point de contact précis pour les dirigeants principaux de la sécurité de l'information du secteur privé. Ces améliorations faciliteront le partage de l'information – de façon protégée – tout en nous aidant à gérer les attaques futures, et à les prévenir.***
>
> *Paiements Canada, 28 février 2018*

Par conséquent, le comité recommande que :

> **Le gouvernement fédéral définisse un cadre national pour l'échange rapide et souple d'information sur la cybersécurité et procède aux ajustements législatifs qui seraient requis à la Loi sur la protection des renseignements personnels et à la Loi sur la protection des renseignements personnels et les documents électroniques afin de permettre l'échange d'information sur les cybermenaces entre des entreprises privées et entre le secteur privé, le gouvernement et les organisations internationales pertinentes.**

En plus d'être une mesure de prévention contre les cybermenaces, la communication d'information est également nécessaire si l'on veut tenter d'intenter des poursuites contre les auteurs de tels crimes. Comme les cybercriminels peuvent se trouver n'importe où dans le monde lorsqu'ils commettent leurs infractions, et qu'ils s'attaquent à de nombreuses cibles simultanément, ces poursuites peuvent représenter un important défi. Comme on l'a fait remarquer, souvent, il n'est pas recommandé de demander de l'information dans le cadre d'accords internationaux, comme le Traité d'entraide judiciaire, car il faut parfois

attendre le traitement de ces types de demandes pendant plus d'un an. Le gouvernement doit investir davantage dans les organismes d'application de la loi pour les aider dans les poursuites liées à ces types de crimes, et notamment déterminer s'il y a lieu de modifier la législation canadienne pour accélérer la communication de renseignements avec les autorités policières d'autres pays.

C'est pourquoi le comité recommande que :

> **Le gouvernement fédéral repère les éventuelles lacunes pouvant nuire à l'échange d'information et qu'il détermine la façon dont les organismes d'application de la loi peuvent être dotés des outils nécessaires au partage actif et rapide d'information et collaborer avec les autres administrations pour poursuivre les cybercriminels.**

2. Uniformiser les normes de cybersécurité avec celles des autres secteurs et des autres administrations

> ***Les entreprises doivent fréquemment gérer un ensemble croissant de règlements en matière de cybersécurité qui se chevauchent dans différentes instances. Il faut les harmoniser à l'aide d'un cadre de base.***
>
> *MasterCard, 1er mars 2018*

On a mentionné à plusieurs reprises que le fait d'avoir des normes de cybersécurité harmonisées et constantes entre les divers secteurs et, idéalement, entre les divers pays était l'un des plus sûrs moyens de ralentir la propagation de la cyberattaque.

Il serait particulièrement important de se doter d'un ensemble de normes de cybersécurité uniformes à l'intention des secteurs des infrastructures essentielles. L'adoption de normes cohérentes en matière de cybersécurité orienterait le travail du gouvernement dans la surveillance de la cybersécurité dans ces secteurs et donnerait aux consommateurs l'assurance que ces systèmes sont protégés.

Certains témoins ont indiqué que les normes minimales en matière de cybersécurité devraient être étendues à toutes les entreprises exerçant des activités dans un secteur d'infrastructure essentielle. Par exemple, à l'égard du secteur financier, on a souligné que, même si les banques bénéficient de la connaissance et de l'expérience nécessaires pour lutter contre les cyberattaques, les nouveaux venus dans le secteur, comme les sociétés de technologie financière, risquent d'avoir des pratiques de cybersécurité moins rigoureuses, ce qui les rend vulnérables pour le secteur. Cependant, les récentes cyberattaques contre la Banque de Montréal et la Simplii Financial, une filiale de la Banque Canadienne Impériale de Commerce, envoient le message selon lequel même les entreprises les plus réglementées, et sans doute dotées des meilleurs moyens de défense contre les attaques

en matière de cybersécurité, ont leurs faiblesses. Par conséquent, les membres du comité sont d'avis que des normes minimales de cybersécurité doivent être élaborées et appliquées à toutes les entreprises au sein des secteurs des infrastructures essentielles.

> ***Le degré élevé d'interconnexion implique qu'une seule attaque contre une institution financière pourrait se propager au système en entier. Par conséquent, les cybermenaces sont devenues une des plus grandes vulnérabilités que les participants au système financier et les autorités de réglementation devront prendre en considération pendant encore longtemps.***
>
> *Banque du Canada, 28 février 2018*

On peut obtenir les conseils voulus pour établir ces normes auprès des pays qui sont des chefs de file sur le plan de la cybersécurité. Des témoins ont mentionné en particulier le Règlement général sur la protection des données (RGPD) de l'Union européenne et le National Institute for Standards and Technology des États-Unis : le RGPD pour ses règles concernant la protection des renseignements personnels saisis, leur stockage, à leur utilisation et leur communication par les entreprises, et le National Institute for Standards pour son expertise technologique.

> ***La portée mondiale croissante des fournisseurs de services financiers - qu'il s'agisse d'importantes institutions financières ou de fournisseurs de services de transfert d'argent sur Internet - signifie qu'un maillon faible de la chaîne peut entraîner un risque au système financier dans son ensemble, si ce dernier n'est pas bien gouverné et coordonné.***
>
> *Ministère des Finances du Canada, 28 février 2018*

Par conséquent, le comité recommande que :

> **Le gouvernement fédéral élabore un ensemble cohérent de normes de haut niveau en matière de cybersécurité qui seraient harmonisées avec les normes internationales les plus élevées et qui s'appliqueraient à toutes les entités participant aux secteurs d'infrastructures essentielles.**

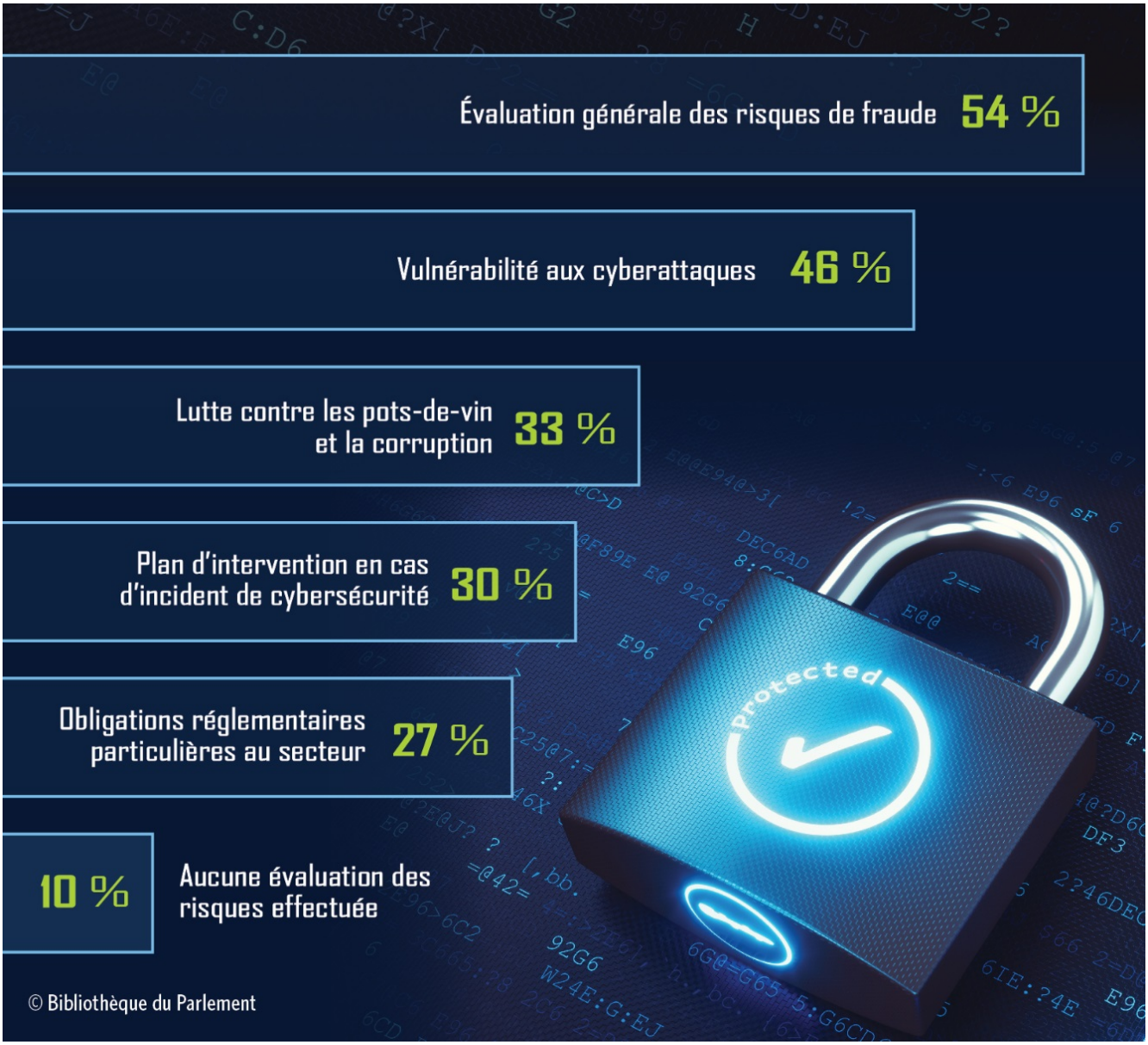
3. Accorder aux entreprises des incitatifs fiscaux à investir dans la cybersécurité

Le secteur privé a besoin de plus de professionnels de la cybersécurité. Cependant, il semble que les entreprises hésitent à investir pour améliorer leurs pratiques en matière de cybersécurité si une de cyberattaque n'a pas d'effets à long terme sur le cours des actions ou sur le comportement de ses consommateurs. Un sondage mené en 2017 par la Chambre de commerce du Canada a révélé que 64 % des entreprises sondées n'avaient pas l'intention d'investir dans des mesures de cybersécurité à ce moment-là, et que 55 % des petites entreprises et 74 % des microentreprises ne prévoyaient effectuer aucun investissement dans la formation sur la cybersécurité au cours d'une période de trois ans.

Comme l'illustre la figure 7, PricewaterhouseCoopers a révélé que 46 % seulement des entreprises ayant participé à son sondage mondial avaient mené une enquête sur les risques de cyberattaque au cours des deux dernières années, et que seulement 30 % d'entre elles avaient mis en place un plan d'intervention de cybersécurité.

Selon le comité, les petites entreprises des secteurs des infrastructures essentielles qui n'ont adopté aucune pratique de cybersécurité suscitent de vastes inquiétudes. Pour les aider, le gouvernement fédéral devrait songer à aider le secteur privé à supporter les dépenses liées à la cybersécurité, notamment en leur accordant à l'égard de celles-ci une déduction pour amortissement accéléré sous le régime de la *Loi de l'impôt sur le revenu*.

Figure 7 - Pourcentage d'entreprises qui ont réalisé des évaluations des risques particulières, 2016 2018, à l'échelle mondiale



Source : PricewaterhouseCoopers, Pulling fraud out of the Shadow – Global Economic Crime and Fraud Survey 2018 [EN ANGLAIS SEULEMENT], p. 7

Par conséquent, le comité recommande que :

> **Le gouvernement fédéral offre des incitatifs aux entreprises, en particulier à celles oeuvrant dans les secteurs des infrastructures essentielles, pour qu'elles puissent améliorer leurs pratiques en matière de cybersécurité, notamment en leur accordant des déductions pour amortissement accéléré pour les investissements dans la cybersécurité au titre de la *Loi de l'impôt sur le revenu*.**

4. S'assurer que les entreprises respectent les lois canadiennes relatives à la protection de la vie privée

> ***Les cyberattaques peuvent frapper des organisations de toute taille et donner lieu à de graves atteintes à la vie privée. Dans le cas des grandes organisations, les vastes banques de données sur leurs clients peuvent présenter un grand intérêt pour les criminels. L'économie numérique actuelle, les petites organisations et les micro-organisations peuvent, elles aussi, détenir de vastes quantités de renseignements personnels. Il se peut aussi qu'elles soient particulièrement vulnérables, car elles peuvent être ciblées par des criminels qui s'attaqueront ensuite à des organisations plus grandes ou partenaires.***
>
> *Commissariat à la protection de la vie privée du Canada, 2 novembre 2017*

Les données présentent une immense valeur, et la protection de ces ressources contre les cyberattaques devrait donc être une priorité absolue pour les entreprises et les gouvernements.

Le RGPD de l'Union européenne est considéré comme ayant les normes les plus élevées relatives aux lois sur la protection des renseignements personnels. Il fait en sorte que les entreprises respectent ses règlements en imposant à celles qui ne le font pas des amendes pouvant atteindre 4 % de leur revenu annuel ou 20 millions d'euros, selon le plus élevé des deux montants.

Le BSFI [Bureau du surintendant des institutions financières] s'attend à ce que les plus grandes institutions financières l'informent des cyberincidents importants dont elles ont eu connaissance, même s'ils n'ont pas provoqué de perturbation observable telle qu'une panne des services en ligne. Nous nous concentrons sur les cyberincidents importants, car ils risquent de perturber le secteur financier

Bureau du surintendant des institutions financières, 28 février 2018

En 2015, on a apporté quelques changements à la LPRPDE pour que celle-ci tienne compte de l'économie numérique, comme la déclaration obligatoire par les entreprises des atteintes à la sécurité des données, qui entrera en vigueur en novembre 2018; cependant, le commissaire à la protection de la vie privée a signalé que le Commissariat ne s'était pas vu accorder de ressources supplémentaires pour traiter ces déclarations. Des études parlementaires récentes ont permis de déterminer qu'à l'ère des progrès rapides de la technologie, les lois canadiennes en matière de protection des renseignements personnels peuvent devoir être revues et modernisées. Dans leurs rapports récents, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes et le Comité sénatorial permanent des transports et des communications ont recommandé au gouvernement fédéral d'apporter aux lois canadiennes relatives à la protection des renseignements personnels des modifications dont l'objectif serait de renforcer la cybersécurité des nouveaux dispositifs technologiques et de donner au commissaire à la protection de la vie privée des pouvoirs d'exécution, notamment ceux de rendre des ordonnances et d'imposer des amendes en cas de non-conformité.

Avant de laisser les consommateurs poursuivre de grandes entreprises à titre individuel, ce qui risque d'être un combat inégal, il pourrait être intéressant de transmettre aux grandes et aux petites entreprises des attentes plus claires et des directives plus explicites sur les niveaux de sécurité auxquels on s'attend de leur part. À partir de là, si elles ne mettent pas en place les mesures nécessaires, on pourra ensuite, éventuellement, envisager des pénalités ou autoriser des poursuites si on se rend compte qu'elles n'ont pas fait le strict nécessaire.

Réseau intégré sur la cybersécurité (SERENE-RISC) 19 octobre 2017

Le comité accepte ces recommandations. Compte tenu du contexte actuel d'économie numérique, toutes les entreprises devraient comprendre combien il importe de protéger leurs systèmes et leurs réseaux et savoir qu'il existe des lois exigeant qu'elles protègent les renseignements des consommateurs. En outre, le gouvernement fédéral doit s'assurer que, lorsque ces entreprises décident de ne pas rendre leurs systèmes cybersécuritaires, le Commissariat à la protection de la vie privée a les pouvoirs et les ressources nécessaires pour faire en sorte qu'elles respectent la loi.

Pour ces raisons, le comité recommande que :

> **Le gouvernement fédéral modernise les lois canadiennes sur la protection des renseignements personnels afin de tenir compte des préoccupations émergentes en matière de cybersécurité et des normes internationales. Il devrait fournir au Commissariat à la protection de la vie privée de nouvelles ressources pour lui permettre de s'acquitter de son mandat, et conférer au commissaire le pouvoir de rendre des ordonnances et d'imposer des amendes aux entreprises qui ne prennent pas les mesures adéquates pour protéger les renseignements de leurs clients.**

C. Améliorer le cadre de cybersécurité du Canada

Dans sa stratégie nationale de cybersécurité de 2018, le gouvernement fédéral a souligné qu'il jouerait un rôle de chef de file dans la promotion de la cybersécurité au Canada. Plus précisément, il y prévoit un « point de convergence clair » pour la cybersécurité, à savoir le nouveau Centre canadien pour la cybersécurité, établi au sein du Centre de la sécurité des télécommunications.

Plusieurs témoins ont suggéré au comité de désigner un organisme responsable de la cybersécurité au sein du gouvernement fédéral, car, dans la stratégie de 2010 en matière de cybersécurité, les mesures de surveillance étaient fragmentées entre plusieurs ministères et organismes fédéraux. La stratégie de 2018 semble regrouper des responsabilités en matière de surveillance de la cybersécurité.

> ***Les joueurs veulent que l'État fédéral se charge d'un rôle de premier plan à l'échelle nationale et sur la scène internationale, pour favoriser la collaboration entre les spécialistes de la cybersécurité, diriger les investissements vers l'industrie de la cybersécurité, faciliter la mise en commun de l'information et sauvegarder les droits et libertés dans le cyberespace.***
>
> *Ministère de la Sécurité publique et de la Protection civile du Canada, 21 mars 2018*

Néanmoins, il reste difficile de savoir quel ministre agirait à titre de responsable principal, soit le ministre de la Sécurité publique et de la Protection civile, qui demeure responsable de la politique nationale en matière de cybersécurité, ou celui de la Défense nationale, qui exerce un rôle de surveillance à l'égard du Centre de la sécurité des télécommunications.

Les membres du comité estiment qu'il serait possible de clarifier le rôle de chef de file du gouvernement fédéral.

Il faudrait créer un nouveau ministère fédéral de la cybersécurité, qui s'acquitterait de certaines des responsabilités relevant actuellement du ministre de la Sécurité publique et de la Protection civile et qui serait responsable de tous les aspects de la cybersécurité, des menaces à la sécurité nationale à l'infrastructure essentielle, en passant par la protection des Canadiens en ligne. Le ministre serait appelé à coordonner les démarches des gouvernements provinciaux et territoriaux de même que celles du secteur privé et des consommateurs en ce qui touche la cybersécurité.

> ***En regroupant sous un même toit la cyberexpertise opérationnelle du gouvernement fédéral, le nouveau centre permettra au gouvernement du Canada de disposer d'une source unifiée de conseils, d'orientations, de services et de soutien spécialisés concernant les questions opérationnelles liées à la cybersécurité. Ainsi, les citoyens et les entreprises du Canada pourront compter sur une source bien établie et fiable vers laquelle de conseils en matière de cybersécurité.***
>
> *Le Centre de la sécurité des télécommunications, 21 mars 2018*

On a signalé que, dans les pays qui sont des chefs de file en matière de cybersécurité, le chef de l'État est l'entité responsable de la cybersécurité, et le Cabinet du premier ministre ou du président coordonne les efforts en matière de cybersécurité. La raison pour laquelle il semble que cette approche soit efficace est que la cybersécurité touche tous les ministères et les organismes relevant du gouvernement fédéral, et qu'un leadership des chefs de gouvernement dans ce dossier fait en sorte que celui-ci reçoit toute l'attention qu'il mérite. Les membres du comité proposent que, jusqu'à ce qu'un nouveau ministère soit créé, l'entité chargée des enjeux liés à la cybersécurité se rapporte directement au Cabinet du premier ministre.

Dans cette optique, le comité recommande que :

> **Le gouvernement fédéral crée un nouveau ministère fédéral de la cybersécurité, qui serait responsable de la politique en matière de cybersécurité, dont la stratégie nationale en matière de cybersécurité, et superviserait le nouveau Centre canadien pour la cybersécurité et l'Unité nationale de coordination de la lutte contre la cybercriminalité.**
>
> **D'ici à ce qu'un tel ministère soit créé, la personne désignée comme étant le chef de file du gouvernement fédéral en cybersécurité devrait relever directement du premier ministre sur les questions en la matière.**
>
> **Enfin, le premier ministre devrait déposer chaque année devant le Parlement un rapport sur les questions relatives à la stratégie de cybersécurité du Canada.**

Compte tenu de l'évolution rapide de la technologie et des diverses formes de cyberattaques, le ministre de la cybersécurité devrait se faire conseiller par des experts en cybersécurité. Un groupe de travail semblable à celui créé par la Maison-Blanche en 2016 devrait être chargé de formuler des recommandations au ministre à propos de la stratégie nationale de cybersécurité, notamment sur la manière de renforcer l'économie numérique du Canada par la cybersécurité et sur la protection des consommateurs et des réseaux d'infrastructures essentielles.

Par conséquent, le comité recommande que :

> **Le gouvernement fédéral crée un groupe fédéral d'experts sur la cybersécurité chargé de formuler des recommandations pour la stratégie nationale de cybersécurité qui feraient du Canada un chef de file mondial en cybersécurité.**

Dans la stratégie, on s'attarde entre autres au rôle du gouvernement fédéral dans la protection de ses systèmes contre les cyberattaques.

Le gouvernement fédéral n'est pas à l'abri des cybermenaces. De graves problèmes de cybersécurité ont été découverts dans divers ministères et organismes gouvernementaux, y compris l'Agence du revenu du Canada, Statistique Canada, le Conseil national de recherches du Canada et Services publics et Approvisionnement Canada. Le commissaire à la protection de la vie privée a constaté que la *Loi sur la protection des renseignements personnels* n'exige pas des ministères et des organismes fédéraux qu'ils déclarent les

atteintes à la vie privée au Commissariat. Or, à compter du 1er novembre 2018, la LPRPDE exigera des entreprises du secteur privé qu'elles déclarent toute atteinte au commissaire à la protection de la vie privée et qu'elles en informent leurs clients « s'il est raisonnable de croire, dans les circonstances, que l'atteinte présent un risque réel de préjudice grave » à leur endroit.

Compte tenu du nombre de renseignements personnels recueillis par le gouvernement fédéral auprès des Canadiens, le commissaire a suggéré que, lorsque leurs données sont violées, les institutions fédérales soient assujetties aux mêmes exigences en matière de production de rapports que les entreprises du secteur privé.

On a également proposé que le gouvernement fédéral déploie plus d'efforts pour sensibiliser les fonctionnaires et les parlementaires aux risques associés à l'utilisation d'appareils pour se connecter à Internet, surtout en voyage à l'étranger. On pourrait créer des pratiques exemplaires pour exiger des fonctionnaires qu'ils utilisent des dispositifs différents pour différents usages. Par exemple, quand un fonctionnaire voyage à l'étranger, il devrait utiliser un appareil plus sécuritaire contre les cybermenaces, même si cet appareil est moins pratique pour lui.

Les membres du comité conviennent que cela aiderait les fonctionnaires fédéraux à comprendre combien il importe de protéger les systèmes du gouvernement contre les cybermenaces. Il devrait être obligatoire d'informer le Commissariat à la protection de la vie privée et le public des atteintes à la protection des renseignements personnels faisant partie du gouvernement, car cela révélerait la mesure de protection des systèmes contre les menaces et éveillerait l'attention des Canadiens sur le fait que des renseignements personnels les concernant peuvent être transmis à des cybercriminels afin que ceux-ci puissent prendre des mesures pour se protéger.

En conséquence, le comité recommande que :

Le gouvernement fédéral enjoigne à ses ministères et à ses organismes de déclarer les atteintes à la vie privée au Commissariat à la protection de la vie privée;

Le gouvernement fédéral continue de mettre en œuvre des pratiques exemplaires à l'intention de la fonction publique fédérale pour garantir l'utilisation de dispositifs sécurisés empêchant la divulgation de renseignements de nature délicate.

CONCLUSIONS DU COMITÉ

Les nouvelles technologies et applications constituent le fondement de la nouvelle économie du Canada et de l'économie de demain. Pour cette raison, le gouvernement fédéral doit agir maintenant pour sensibiliser les Canadiens au fait que nous avons un rôle commun à jouer dans la protection de notre pays contre les cybermenaces, qui évoluent sans cesse. Que ce soit par l'acquisition de nouvelles compétences pour pouvoir travailler dans le domaine de la cybersécurité, la participation à la recherche et au développement en cybersécurité ou tout simplement l'apprentissage de la façon de veiller à la sécurité des renseignements personnels qu'ils détiennent dans le cyberespace, tous les Canadiens doivent apprendre comment ils peuvent participer à la lutte contre la cybercriminalité.

Autrefois, seuls les experts de la technologie se préoccupaient de la cybersécurité et de la protection des renseignements personnels : aujourd'hui, c'est tout le monde des affaires et l'ensemble de la société qui s'en inquiètent. La cybersécurité n'est plus un simple problème de TI : c'est un problème opérationnel qui touche tout le monde. Ce ne sont plus les appareils qui constituent le maillon faible de la chaîne en matière de sécurité, mais bien les utilisateurs. Ainsi, on considère maintenant que le facteur humain représente la plus grande menace à la cybersécurité.

Institut canadien de la cybersécurité, Université du Nouveau-Brunswick, 29 mars 2018

Les entreprises détiennent des quantités considérables de renseignements personnels parce que leurs clients comptent sur elles pour qu'ils demeurent confidentiels. Elles doivent être informées au sujet des cybermenaces nouvelles et existantes, et apprendre à bien protéger leurs systèmes. Le commissaire à la protection de la vie privée devrait avoir le pouvoir de s'assurer que tout manquement au devoir de protéger les renseignements personnels des Canadiens soit lourd de conséquences.

Enfin, les ministères, les organismes et les systèmes gouvernementaux sont souvent la cible de cybercriminels, et, lorsque cela se produit, il faut que les Canadiens le sachent. Il reste encore beaucoup à faire pour s'assurer que les Canadiens savent où chercher de l'aide en cas de cyberattaque. La création d'un nouveau ministre de la cybersécurité, s'appuyant sur des spécialistes en cybersécurité, permettrait d'y parvenir.

La cybersécurité est un grave problème qui ne peut être résolu que si les Canadiens, les entreprises et les gouvernements collaborent pour y trouver des solutions.

ANNEXE A : TÉMOINS AYANT COMPARU DEVANT LE COMITÉ

Le 18 octobre 2017

Gendarmerie royale du Canada
Surintendant principal Scott Doran, directeur général, Opérations criminelles de la Police fédérale
Surintendant Mark Flynn, directeur, Cybercriminalité, Police fédérale

Sécurité publique Canada
Adam Hatfield, directeur général par intérim, Direction de la cybersécurité nationale

Service canadien du renseignement de sécurité
Charles Lowson, directeur général, Contre-espionnage et Lutte contre la prolifération

Le 19 octobre 2017

Centre de la sécurité des télécommunications
André Boucher, directeur général, Partenariats en cybersécurité
Scott Jones, chef adjoint, Sécurité des TI

Réseau intégré sur la cybersécurité (SERENE-RISC)
Benoît Dupont, directeur scientifique

Le 26 octobre 2017

Association des banquiers canadiens
Darren Hannah, vice-président, Finances, risques et politique prudentielle
Andrew Ross, directeur, Paiements et cybersécurité
Sandy Stephens, avocate-conseil adjointe

Le 2 novembre 2017

Commissariat à la protection de la vie privée du Canada
Daniel Therrien, commissaire à la protection de la vie privée
Brent Homan, directeur général, Direction des enquêtes liées à la Loi sur la protection des renseignements personnels et les documents
Steven Johnston, analyste principal de recherche en TI
Patricia Kosseim, avocate générale principale et directrice générale, Direction des services juridiques, des politiques, de la recherche et de l'analyse des technologies

Le 28 février 2018

Banque du Canada
Ron Morrow, directeur général, Département de la Stabilité financière

Bureau du surintendant des institutions financières
Judy Cameron, directrice principale, Législation, approbations et politique stratégique
Theresa Hinz, directrice, Approbations et précédents

Ministère des Finances Canada
Annette Ryan, sous-ministre adjointe déléguée, Direction de la politique du secteur financier

Paiements Canada
Justin Ferrabee, chef des opérations
Martin Kyle, dirigeant principal de la sécurité de l'information

Le 1 mars 2018
Échange canadien de menaces cybernétiques
Robert W. Gordon, directeur général

La Chambre de commerce du Canada
Scott Smith, directeur, Propriété intellectuelle et politique d'innovation

Mastercard
Ron Green, chef de la sécurité

Le 21 mars 2018
Centre de la sécurité des télécommunications
André Boucher, chef adjoint associé, Sécurité des TI

Gendarmerie royale du Canada
Surintendant principal Jeff Adam, commissaire adjoint, Opérations techniques

Institut de la cybersécurité et de la protection des renseignements personnels (Université de Waterloo)
Florian Kerschbaum, directeur intérimaire

Sécurité publique Canada
Colleen Merchant, directrice générale, Direction de la cybersécurité nationale

Le 22 mars, 2018
Morrison & Foerster s.r.l.
John P. Carlin, président, Risques mondiaux et gestion de crise

Le 28 mars, 2018
Institut canadien de la cybersécurité (Université du Nouveau-Brunswick)
Ali Ghorbani, directeur

ANNEXE B : MÉMOIRES

Commissariat à la protection de la vie privée du Canada
Daniel Therrien, commissaire à la protection de la vie privée