Nº 85-002-X au catalogue
ISSN 1205-8882

Juristat

Les défis des entreprises canadiennes quant à la cybersécurité et au cybercrime, 2017

par Howard Bilodeau, Mohammad Lari et Mark Uhrbach
Centre canadien de la statistique juridique

Date de diffusion : le 28 mars 2019

Statistique Canada Statistics Canada

Canada

Comment obtenir d'autres renseignements

Pour toute demande de renseignements au sujet de ce produit ou sur l'ensemble des données et des services de Statistique Canada, visiter notre site Web à www.statcan.gc.ca.

Vous pouvez également communiquer avec nous par :

courriel à STATCAN.infostats-infostats.STATCAN@canada.ca

téléphone entre 8 h 30 et 16 h 30 du lundi au vendredi aux numéros suivants :

- Service de renseignements statistiques 1-800-263-1136
- Service national d'appareils de télécommunications pour les malentendants 1-800-363-7629
- Télécopieur 1-514-283-9350

Programme des services de dépôt

- Service de renseignements 1-800-635-7943
- Télécopieur 1-800-565-7757

Normes de service à la clientèle

Statistique Canada s'engage à fournir à ses clients des services rapides, fiables et courtois. À cet égard, notre organisme s'est doté de normes de service à la clientèle que les employés observent. Pour obtenir une copie de ces normes de service, veuillez communiquer avec Statistique Canada au numéro sans frais 1-800-263-1136. Les normes de service sont aussi publiées sur le site www.statcan.gc.ca sous « Contactez-nous » > « Normes de service à la clientèle ».

Note de reconnaissance

Le succès du système statistique du Canada repose sur un partenariat bien établi entre Statistique Canada et la population du Canada, les entreprises, les administrations et les autres organismes. Sans cette collaboration et cette bonne volonté, il serait impossible de produire des statistiques exactes et actuelles.

Les défis des entreprises canadiennes quant à la cybersécurité et au cybercrime, 2017 : faits saillants

- Un peu plus du cinquième (21 %) des entreprises canadiennes ont déclaré avoir été touchées par des incidents de cybersécurité qui ont eu des répercussions sur leurs activités en 2017, comparativement à 23 % des entreprises au Royaume-Uni.
- Plus de la moitié (54 %) des entreprises touchées par des incidents de cybersécurité au Canada ont déclaré que ces derniers avaient empêché les employés d'effectuer leurs tâches quotidiennes, tandis que près du tiers (30 %) ont dit que ces incidents avaient entraîné des frais de réparation ou de rétablissement supplémentaires.
- Environ 10 % des entreprises au Canada ont déclaré avoir perdu des revenus en raison d'incidents de cybersécurité, et une plus petite proportion (6 %) des entreprises ont mentionné que les incidents avaient nui à la réputation de leur entreprise.
- Les entreprises qui ont déclaré le plus grand nombre d'incidents de cybersécurité au Canada sont les établissements bancaires (à l'exclusion des services bancaires d'investissement) (47 %), les universités (46 %) et les entreprises du transport par pipeline (45 %). En 2017, les entreprises de ces secteurs ont été principalement touchées par des incidents dont le motif était de voler de l'argent ou de demander le paiement d'une rançon.
- Pour tous les types d'incidents survenus en 2017, 65 % des entreprises canadiennes ont déclaré soupçonner qu'un tiers était responsable des incidents de cybersécurité.
- Environ 10 % des entreprises canadiennes touchées par un incident de cybersécurité ont signalé l'incident à un service de police en 2017.
- En 2017, la grande majorité (94 %) des entreprises canadiennes ont engagé un certain niveau de dépenses pour prévenir et détecter les incidents de cybersécurité. En moyenne, les entreprises canadiennes ont dépensé 78 000 $ à ces fins. Les grandes entreprises ont engagé les dépenses les plus élevées (dépenses moyennes de 922 000 $), suivies des moyennes entreprises (dépenses moyennes de 108 000 $). Les petites entreprises ont déclaré avoir dépensé en moyenne 44 000 $.
- La majorité des grandes (91 %), des moyennes (83 %) et des petites (72 %) entreprises au Canada ont déclaré avoir des employés principalement responsables de la cybersécurité générale de l'entreprise en 2017. De plus, bon nombre d'entre elles ont aussi eu recours à des experts-conseils ou à des entrepreneurs pour gérer les risques et les menaces liés à la cybersécurité. Environ 45 % des moyennes entreprises ont eu recours à des services d'experts-conseils et d'entrepreneurs, comparativement à 38 % des grandes entreprises et à 33 % des petites entreprises.
- Très peu (5 %) d'entreprises canadiennes ont déclaré ne pas avoir de mesures de cybersécurité en place pour se protéger ainsi que pour protéger leurs clients et leurs partenaires. Outre les mesures de cybersécurité en place, plus de la moitié (58 %) des entreprises ont mis en œuvre des activités pour cerner les risques liés à la cybersécurité.

Les défis des entreprises canadiennes quant à la cybersécurité et au cybercrime, 2017

par Howard Bilodeau, Mohammad Lari et Mark Uhrbach

Les entreprises canadiennes continuent rapidement d'accroître l'utilisation d'Internet et de technologies numériques, ce qui peut les exposer à des risques et des menaces accrus en matière de cybersécurité. Toutefois, il est difficile de saisir l'incidence qu'ont ces risques et ces menaces sur les investissements et les décisions quotidiennes des entreprises, puisque les incidents de cybersécurité ne sont pas toujours signalés (van der Meer, 2015).

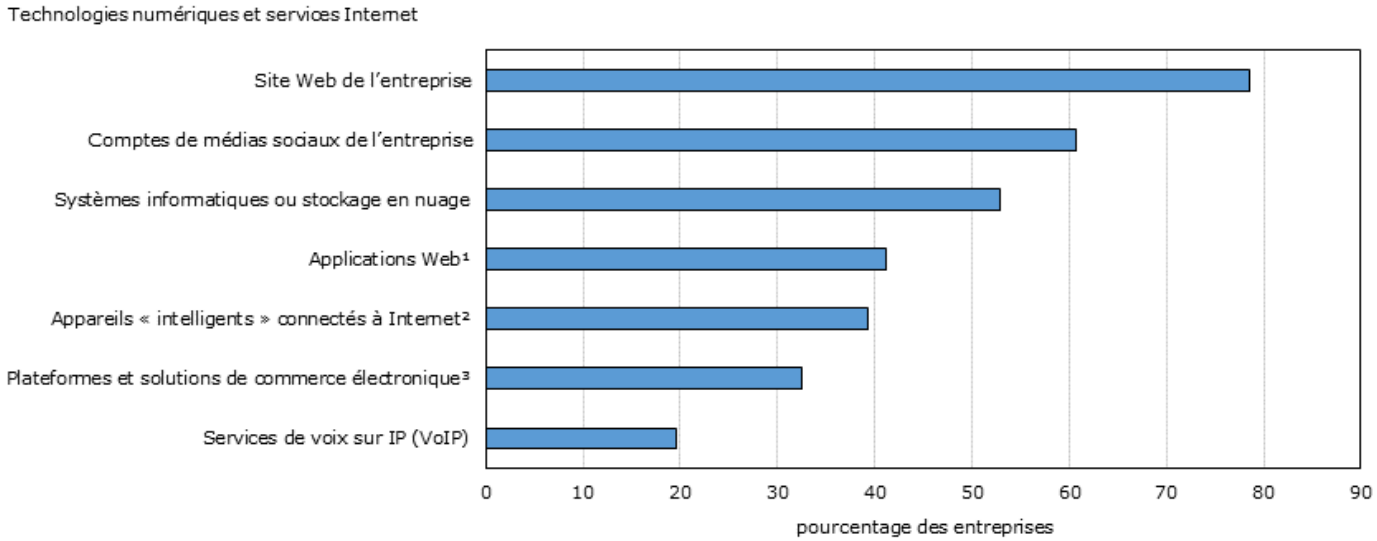
Le présent article de *Juristat* est fondé sur les renseignements recueillis dans le cadre de l'Enquête canadienne sur la cybersécurité et le cybercrime (ECCC), la première enquête statistique officielle de ce genre au Canada. Il traite de certaines lacunes statistiques et fournit des renseignements nouveaux et actuels sur le comportement des entreprises canadiennes confrontées aux défis de cybersécurité d'un monde en évolution[1].

Tout d'abord, cet article porte sur la façon dont les entreprises sont exposées aux risques et aux menaces liés à la cybersécurité en raison de leur utilisation des technologies et des services numériques connectés à Internet. Ensuite, il aborde les répercussions du cybercrime sur les activités des entreprises en 2017 ainsi que leurs pratiques de signalement après un incident. Enfin, il traite des types d'investissements effectués par les entreprises pour gérer ces risques et ces menaces en fonction des types de mesures de cybersécurité qu'elles utilisent.

La grande majorité des entreprises dépendent des technologies et des services numériques

La dépendance croissante des entreprises aux technologies et aux services numériques connectés à Internet les expose à de plus grands risques en matière de cybersécurité. Environ 92 % des entreprises canadiennes ont déclaré avoir utilisé un ou plusieurs services ou technologies numériques en 2017[2]. Plus précisément, près de 80 % des entreprises avaient un site Web en 2017 et 61 % avaient un compte de médias sociaux. L'utilisation de ces technologies semble avoir augmenté considérablement depuis 2013, alors que 46 % des entreprises avaient déclaré avoir un site Web, et environ 38 % d'entre elles l'avaient relié à leurs comptes de médias sociaux (Statistique Canada, 2013a; Statistique Canada, 2013b)[3]. En outre, une grande proportion des entreprises utilisent également d'autres technologies, comme les services d'informatique et de stockage en nuage (53 %) ainsi que les appareils « intelligents » connectés à Internet (39 %) (graphique 1).

Graphique 1
Types de technologies numériques et de services Internet utilisés, Canada, 2017



1. Par exemple, le traitement de la paye, la signature électronique, les demandes de service de commande et de livraison.
2. Par exemple, les télévisions intelligentes et les caméras de sécurité compatibles à la technologie Wi-Fi.
3. Par exemple, le paiement et la commande en ligne.

Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime.

À mesure que la dépendance aux technologies et aux services numériques connectés à Internet et connectés les uns aux autres continue de croître, le risque que ces technologies et ces services soient manipulés par des tiers non autorisés augmente proportionnellement (van der Meer, 2015). Les cybercriminels sont capables de tirer profit du rythme rapide des progrès technologiques en exploitant les vulnérabilités et les lacunes de sécurité dans l'infrastructure cybernétique.

Le stockage de données sur des services Web hébergés à l'externe (comme le stockage en nuage) peut exposer les entreprises canadiennes à des risques de cybersécurité (Bigo et autres, 2012). En 2017, environ le tiers (31 %) des entreprises utilisaient Internet pour stocker des renseignements confidentiels sur leur entreprise, comme des renseignements relatifs à leur inventaire ou à leurs états financiers, et 30 % des entreprises y stockaient des renseignements confidentiels concernant leurs clients, leurs fournisseurs ou leurs partenaires. Malgré cela, plus de la moitié (54 %) des entreprises qui utilisaient le stockage en nuage n'avaient pas mis en place leurs propres mesures de protection et de contrôle des données, comme le chiffrement ou la gestion des droits. Ce problème était plus courant chez les petites entreprises (59 %) que chez les grandes (20 %). Dans certains cas, il est possible que ces types de mesures de protection de la sécurité aient été assurés par le fournisseur de services d'informatique en nuage.

Des différences notables ont également été observées entre les secteurs en 2017. Près de 63 % des entreprises d'extraction de pétrole et de gaz[4] ont déclaré utiliser Internet pour stocker des renseignements confidentiels concernant leur entreprise, alors que cette proportion était beaucoup plus faible (15 %) dans le cas des hôpitaux[5].

Les entreprises les plus susceptibles d'utiliser Internet pour stocker des renseignements confidentiels concernant leurs clients, leurs fournisseurs ou leurs partenaires en 2017 étaient les agences de presse, les bibliothèques et les archives, les entreprises d'édition, de radiodiffusion et de télédiffusion par Internet et les sites portails de recherche[6] (67 %); les entreprises de distribution de gaz naturel[7] (65 %); et les établissements bancaires[8], à l'exclusion des services bancaires d'investissement (61 %). Ce mode de gestion de l'information pourrait éventuellement avoir des conséquences pour certaines entreprises, car les cybercriminels continuent de parfaire leurs moyens d'accéder aux systèmes de stockage de données personnelles et financières des clients (Bigo et autres, 2012).

Les deux tiers des entreprises permettent à leurs employés d'utiliser des appareils personnels à des fins professionnelles

Lorsque les entreprises permettent à leurs employés d'utiliser des appareils personnels à des fins professionnelles, elles s'exposent aux attaques de cybersécurité. La vulnérabilité des appareils personnels pourrait s'étendre au réseau de l'entreprise et le compromettre, et vice versa (Commissariat à la protection de la vie privée du Canada, 2015).

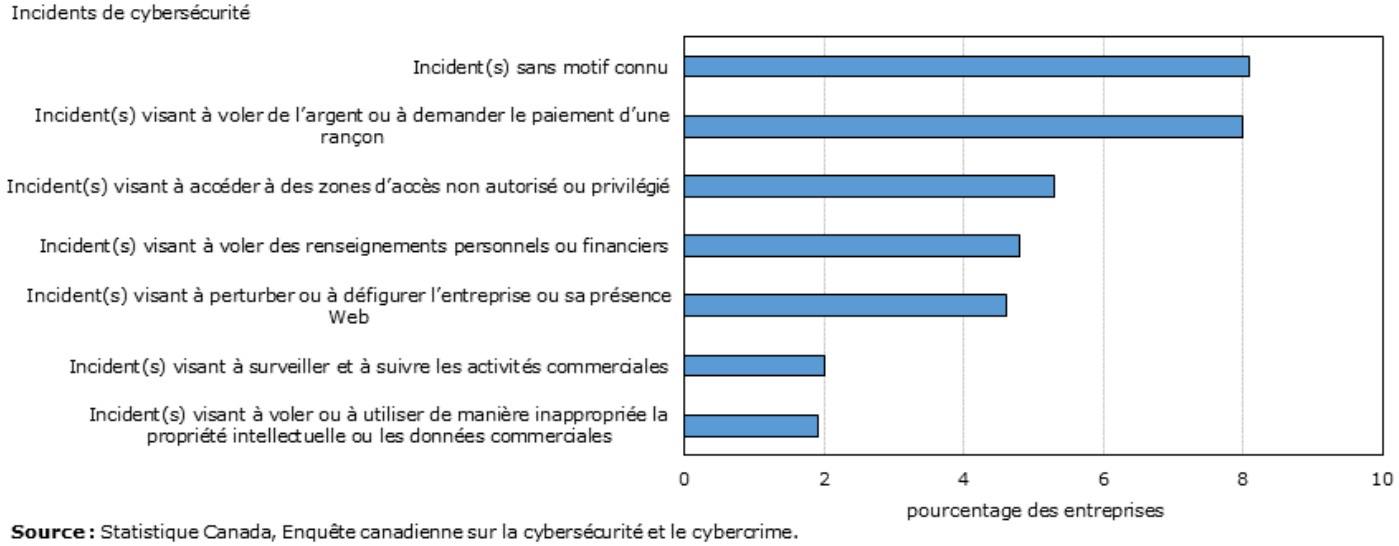
En 2017, les deux tiers (66 %) des entreprises permettaient à leurs employés d'utiliser des appareils personnels pour mener des activités liées à l'entreprise, soit une proportion qui était généralement uniforme dans l'ensemble des entreprises de toutes les tailles. Cependant, la majorité (64 %) des petites entreprises (10 à 49 employés) n'avaient pas de mesures de sécurité en place pour gérer l'utilisation des appareils personnels, comparativement à 46 % des moyennes entreprises (50 à 249 employés) et à 21 % des grandes entreprises (250 employés ou plus). Ainsi, les petites entreprises sont probablement plus vulnérables au cybercrime parce qu'elles adoptent des technologies et des services sans mettre en place des mesures de sécurité adéquates.

Un peu plus du cinquième des entreprises canadiennes ont été touchées par des incidents de cybersécurité qui ont eu des répercussions sur leurs activités

En 2017, un peu plus du cinquième (21 %) des entreprises canadiennes ont déclaré avoir été touchées par des incidents de cybersécurité qui ont eu des répercussions sur leurs activités[9]. Environ 19 % des petites entreprises ont déclaré avoir été touchées par de tels incidents, comparativement à 28 % des moyennes entreprises et à 41 % des grandes entreprises.

Parmi les entreprises touchées par des incidents de cybersécurité, 39 % n'ont pas pu déterminer le motif de l'attaque, tandis que 38 % ont déclaré que le motif était une tentative de vol d'argent ou une demande de paiement d'une rançon. Un peu plus du quart (26 %) des entreprises ont été victimes d'incidents où les auteurs ont tenté d'accéder à des zones d'accès non autorisé ou privilégié, alors que 23 % ont été victimes d'incidents où il y a eu tentative de vol de renseignements personnels ou financiers (graphique 2).

Graphique 2
Types d'incidents de cybersécurité ayant eu des répercussions sur les activités des entreprises, Canada, 2017



Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime.

Pour tous les types d'incidents, 65 % des entreprises ont déclaré croire qu'une partie externe était responsable des incidents de cybersécurité. Cependant, les renseignements au sujet de ces cybercriminels sont souvent inconnus, puisque le but des cybercrimes est généralement d'accéder à des ordinateurs ou à des réseaux informatiques en évitant de se faire détecter (van der Meer, 2015).

Les entreprises victimes d'incidents ayant eu des répercussions sur leurs activités en 2017 ont déclaré que ceux-ci avaient été principalement perpétrés au moyen d'arnaques ou de fraude (p. ex. fraude financière ou hameçonnage) et de logiciels malveillants (p. ex. virus, logiciels publicitaires ou logiciels de rançon).

Plus de la moitié (54 %) des entreprises touchées par des incidents de cybersécurité ont déclaré que ces derniers avaient empêché les employés d'effectuer leurs tâches quotidiennes, tandis que près du tiers (30 %) ont affirmé que ces incidents avaient entraîné des frais de réparation ou de rétablissement supplémentaires. Environ 10 % des entreprises ont déclaré avoir perdu des revenus, 6 % ont indiqué que les incidents avaient nui à la réputation de leur entreprise, 4 % ont dû rembourser des tiers ou payer une rançon, et environ 2 % ont perdu des fournisseurs, des clients ou des partenaires en raison d'incidents de cybersécurité en 2017.

La majorité (58 %) des entreprises touchées par des incidents de cybersécurité en 2017 ont connu un temps d'arrêt à la suite de ceux-ci, alors qu'un peu plus du tiers (35 %) des entreprises ont déclaré que les incidents étaient mineurs et qu'ils avaient eu une incidence minime sur leurs activités. En moyenne, le temps d'arrêt total des entreprises canadiennes en 2017 était de 23 heures et touchait les appareils mobiles, les ordinateurs de bureau et les réseaux.

Lorsque l'on compare les risques pris par les entreprises aux taux d'incidents survenus, on constate que les entreprises qui ont stocké des données sur des services Web hébergés à l'externe (p. ex. le stockage en nuage) étaient plus susceptibles que la moyenne d'avoir été victimes d'incidents qui ont eu des répercussions sur leurs activités (26 %). De même, les entreprises qui permettaient l'utilisation d'appareils personnels à des fins professionnelles étaient aussi plus susceptibles que la moyenne d'avoir été touchées par des brèches ayant eu des répercussions sur leurs activités (24 %). Cette tendance a été observée pour l'ensemble des entreprises de toutes les tailles.

À la suite d'un incident de cybersécurité qui a eu des répercussions sur leurs activités, les entreprises étaient plus susceptibles de communiquer avec un expert-conseil ou un entrepreneur en technologie de l'information (51 %) qu'avec d'autres tiers pour obtenir des renseignements ou des conseils. Une proportion de 15 % des entreprises ont communiqué avec un fournisseur de logiciels ou de services, et environ 12 % d'entre elles ont communiqué avec leurs fournisseurs, leurs clients ou leurs partenaires. Les entreprises canadiennes étaient également plus susceptibles d'avoir demandé des renseignements ou des conseils à la communauté Internet (p. ex. forum ou blogue) (10 %) qu'à un service de police (5 %).

Un plus grand nombre d'entreprises des secteurs des infrastructures essentielles ont été touchées par des incidents de cybersécurité qui ont eu des répercussions sur leurs activités, comparativement aux entreprises des autres secteurs

Les entreprises qui ont déclaré le plus grand nombre d'incidents de cybersécurité étaient les établissements bancaires[8] (47 %), les universités[10] (46 %) et les entreprises du transport par pipeline[11] (45 %). En 2017, les entreprises de ces secteurs ont été principalement touchées par des incidents dont le motif était de voler de l'argent ou de demander le paiement d'une rançon.

Un peu plus de la moitié (51 %) des établissements bancaires[8] qui ont été victimes d'incidents de cybersécurité ayant eu des répercussions sur leurs activités en 2017 ont déclaré avoir perdu des revenus en raison de ces derniers, alors que la majorité des universités (70 %) et des entreprises du transport par pipeline (76 %) ont révélé que leurs employés avaient eu besoin de travailler des heures supplémentaires à la suite des incidents.

Bien que les entreprises canadiennes aient dépensé en moyenne 16 000 $ pour se remettre de tous les incidents de cybersécurité qui ont eu des répercussions sur leurs activités en 2017, ces coûts moyens étaient considérablement plus élevés pour les entreprises des secteurs des infrastructures essentielles. Les entreprises du transport par pipeline ont dépensé 131 000 $, suivies des entreprises de distribution de gaz naturel (118 000 $) et des établissements bancaires[8] (87 000 $). En comparaison, les universités (13 000 $) ont dépensé moins que la moyenne.

De plus en plus, les entreprises des secteurs des infrastructures essentielles sont ciblées par les cybercriminels en raison de leur vaste réseau numérique, de leur interconnexion et de leur grande valeur pour la santé, la sécurité et le bien-être économique des Canadiens. Les entreprises de ces secteurs gèrent des biens et des systèmes, comme les chaînes d'approvisionnement alimentaire, les réseaux électriques, l'infrastructure de transport, l'infrastructure des communications et les systèmes de sécurité publique (voir Gendron et Rudner, 2012; Sécurité publique Canada, 2009 pour obtenir plus de renseignements sur les menaces émergentes qui guettent les infrastructures essentielles).

Encadré 1
Mesures et pratiques de cybersécurité des entreprises au Royaume-Uni

Les données comparables sur les mesures et les pratiques de cybersécurité des entreprises se font rares, puisque la majorité des enquêtes réalisées à ce jour sur la scène internationale ne sont pas représentatives de l'ensemble des entreprises. Ces enquêtes comportaient des limites en raison de la petite taille de l'échantillon, du faible taux de réponse et des différences importantes entre les types de questions posées et les concepts de cybersécurité utilisés.

Cela dit, bien que les données de l'Enquête canadienne sur la cybersécurité et le cybercrime et de l'enquête sur les brèches de cybersécurité de 2018 menée au Royaume-Uni présentent des divergences, ces deux enquêtes sont semblables sur le plan du contenu. Par conséquent, certaines comparaisons avec les données recueillies au Royaume-Uni sont incluses dans le présent article afin de vérifier si les entreprises canadiennes ont vécu une expérience semblable à celle des entreprises au Royaume-Uni (voir la section Description de l'enquête pour obtenir une description détaillée de ces enquêtes).

Un nombre légèrement plus élevé d'entreprises au Royaume-Uni ont été victimes d'incidents de cybersécurité ayant eu des répercussions sur leurs activités

Environ 23 %[12] des entreprises au Royaume-Uni[13] ont été victimes d'incidents de cybersécurité ayant eu des répercussions sur leurs activités, et plus des deux tiers (69 %) de ces entreprises ont affirmé avoir eu à mettre en place de nouvelles mesures pour se protéger contre de futures attaques. La majorité (60 %) des entreprises touchées par des incidents de cybersécurité au Royaume-Uni ont déclaré que le personnel avait dû travailler des heures supplémentaires à la suite des incidents, comparativement à près du tiers (32 %) des entreprises canadiennes. Un peu plus de la moitié des entreprises touchées par des incidents de cybersécurité au Royaume-Uni (51 %) et au Canada (54 %) ont mentionné que les incidents ou les attaques liés à la cybersécurité avaient empêché leurs employés d'effectuer leurs tâches quotidiennes.

Les entreprises des deux pays ont également révélé avoir perdu des revenus ou de la valeur en bourse à la suite d'incidents de cybersécurité (8 % des entreprises au Royaume-Uni par rapport à 10 % des entreprises canadiennes), et un plus faible pourcentage d'entreprises des deux pays (6 % dans chaque cas) ont déclaré que les incidents ont nui à leur réputation.

Bien qu'il soit impossible d'effectuer une comparaison directe du temps d'arrêt des activités des entreprises au Canada et au Royaume-Uni à la suite d'incidents de cybersécurité[14], certaines données laissent croire que les incidents de cybersécurité ont eu des répercussions semblables sur le temps d'arrêt des entreprises des deux pays. En effet, la majorité (56 %) des entreprises touchées par des brèches de sécurité ou des attaques au Royaume-Uni ont déclaré avoir eu besoin de temps pour se remettre de leur attaque la plus perturbatrice. Il s'agit d'une proportion semblable à celle observée au Canada, où 58 % des entreprises ont déclaré avoir connu un temps d'arrêt à la suite d'un incident survenu en 2017.

Encadré 1 — fin
Mesures et pratiques de cybersécurité des entreprises au Royaume-Uni

Comme au Canada, les entreprises au Royaume-Uni qui détenaient des données personnelles sur des clients (27 %) et celles qui permettaient l'utilisation d'appareils personnels à des fins professionnelles (27 %) étaient plus susceptibles que la moyenne d'avoir été victimes d'un incident de cybersécurité ayant eu des répercussions sur leurs activités.

Les entreprises au Royaume-Uni ont dépensé en moyenne 5 100 $ pour se remettre d'incidents de cybersécurité, et ce sont les grandes et les moyennes entreprises qui ont engagé les dépenses les plus élevées à cette fin (27 000 $ et 37 000 $, respectivement)[15].

Parmi les entreprises canadiennes touchées par des incidents de cybersécurité, 1 sur 10 a signalé les incidents à un service de police

Parmi les entreprises canadiennes touchées par des incidents de cybersécurité, environ 10 % les ont signalés à un service de police en 2017. Les établissements bancaires[8] étaient de loin les plus susceptibles de signaler un incident ayant eu des répercussions sur leurs activités à un service de police (60 %), suivis des entreprises de production, de transport et de distribution d'électricité[16] (25 %) et des entreprises du transport par pipeline (24 %).

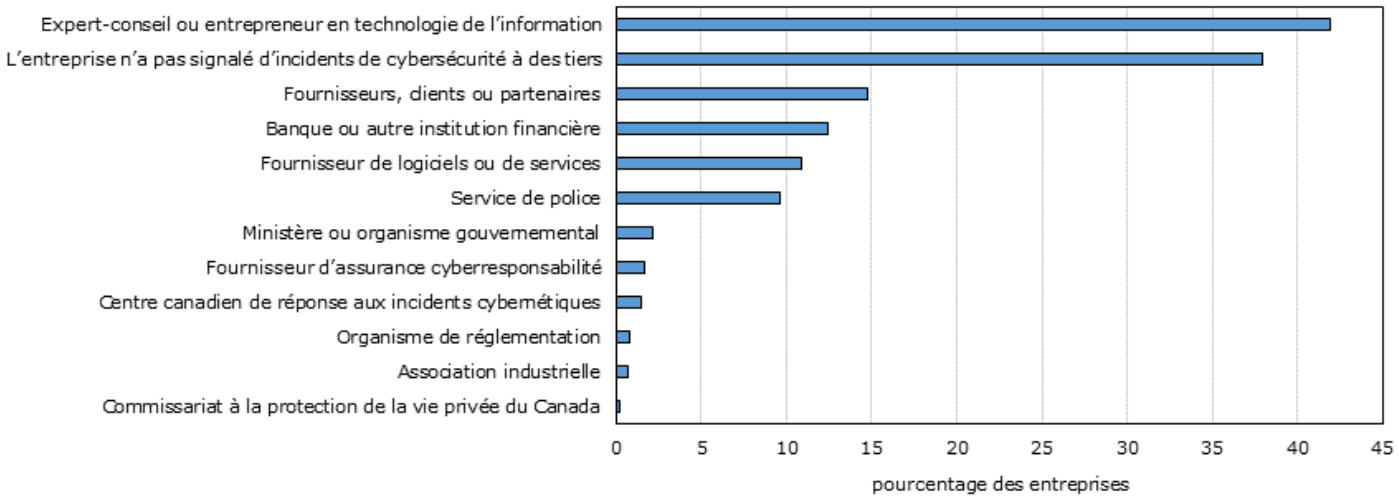
Les taux de signalement plus élevés parmi certains types d'entreprises peuvent s'expliquer en partie par les partenariats entre le gouvernement du Canada et les propriétaires et exploitants d'infrastructures essentielles de ces secteurs. Ces partenariats sont en place pour veiller à la prévention des perturbations des infrastructures essentielles ainsi qu'à la mise en place de mesures d'intervention et de rétablissement en cas de perturbations (Sécurité publique Canada, 2009).

Plus de la moitié (53 %) des entreprises ayant été touchées par des incidents de cybersécurité et qui ne les ont pas signalés à un service de police ont expliqué ne pas l'avoir fait parce qu'ils avaient été résolus à l'interne. Plus du tiers (35 %) des entreprises n'ont pas signalé les incidents parce qu'ils ont été résolus par des experts-conseils ou des entrepreneurs en technologie de l'information (TI), tandis que 29 % d'entre elles n'ont pas signalé les incidents aux services de police parce qu'elles estimaient que les répercussions étaient trop mineures.

Plus du quart (26 %) des entreprises touchées par des incidents de cybersécurité n'ont pas pensé à communiquer avec un service de police et environ 13 % doutaient du fait que l'auteur serait déclaré coupable ou adéquatement puni. Quelques entreprises (4 %) ont trouvé le processus de signalement trop complexe ou nébuleux, ou n'étaient pas satisfaites de la façon dont le service de police avait traité un incident dans le passé (2 %).

Les entreprises touchées par des incidents de cybersécurité ont également signalé ces incidents à leurs fournisseurs, à leurs clients ou à leurs partenaires (15 %), à leurs banques ou autres institutions financières (12 %) et à leurs fournisseurs de logiciels ou de services (11 %) (graphique 3). Très peu (1 %) d'entreprises ont signalé des incidents au Centre canadien de réponse aux incidents cybernétiques (CCRIC). Cependant, les entreprises des secteurs des infrastructures essentielles ont signalé un plus grand nombre d'incidents au CCRIC que les entreprises des autres secteurs. Les entreprises des infrastructures essentielles comprennent les établissements bancaires[8] (52 %), les entreprises de production, de transport et de distribution d'électricité (22 %) et les universités (18 %).

Graphique 3
Tiers à qui les incidents ayant eu des répercussions sur les activités des entreprises ont été signalés, Canada, 2017



Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime.

Plus du tiers (38 %) des entreprises n'ont pas signalé d'incident de cybersécurité ayant eu des répercussions sur leurs activités à une partie externe. Ce résultat est en partie attribuable au fait que peu d'incidents ont été signalés à d'autres ministères ou organismes gouvernementaux (2 %) et au Commissariat à la protection de la vie privée (moins de 1 %). Cela dit, le nombre de signalements au Commissariat à la protection de la vie privée devrait augmenter au fil du temps en raison des nouvelles dispositions législatives qui sont entrées en vigueur en novembre 2018 et qui sont assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques*, lesquelles obligent toutes les entreprises à déclarer les brèches de sécurité touchant des renseignements personnels (Commissariat à la protection de la vie privée du Canada, 2018).

De plus, 36 % des entreprises touchées par des incidents de cybersécurité ont déclaré que les incidents impliquant leur organisation leur avaient été signalés par des tiers. Ces tiers étaient souvent des fournisseurs, des clients ou des partenaires (17 %) et des experts-conseils ou des entrepreneurs en TI (15 %). Près de la moitié (47 %) de ces incidents de cybersécurité ont été résolus à l'interne, et très peu d'entre eux ont été signalés à un service de police (4 %).

Encadré 2
Le taux de signalement d'incidents de cybersécurité à un tiers est plus faible parmi les entreprises au Royaume-Uni que celles au Canada

Environ 47 % des entreprises qui ont été touchées par des brèches de sécurité ou des attaques cybernétiques au Royaume-Uni ont signalé leur brèche la plus perturbatrice à un tiers, tandis que ce pourcentage était de 64 % parmi les entreprises canadiennes touchées par des incidents de cybersécurité (les tiers comprennent les services de police). Au Royaume-Uni, les petites (50 %) et les moyennes (43 %) entreprises étaient plus susceptibles de signaler des incidents de cybersécurité à un tiers que les grandes entreprises (36 %). C'était également le cas au Canada, où 65 % des moyennes entreprises et 64 % des petites entreprises ont signalé des incidents ayant eu des répercussions sur leurs activités à un tiers (y compris les services de police), comparativement à 53 % des grandes entreprises. Dans les deux pays, les différences observées dans les pratiques de signalement selon la taille des entreprises sont en grande partie attribuables au fait qu'un pourcentage plus élevé de petites et de moyennes entreprises signalent les incidents à leur expert-conseil ou à leur entrepreneur externe en TI.

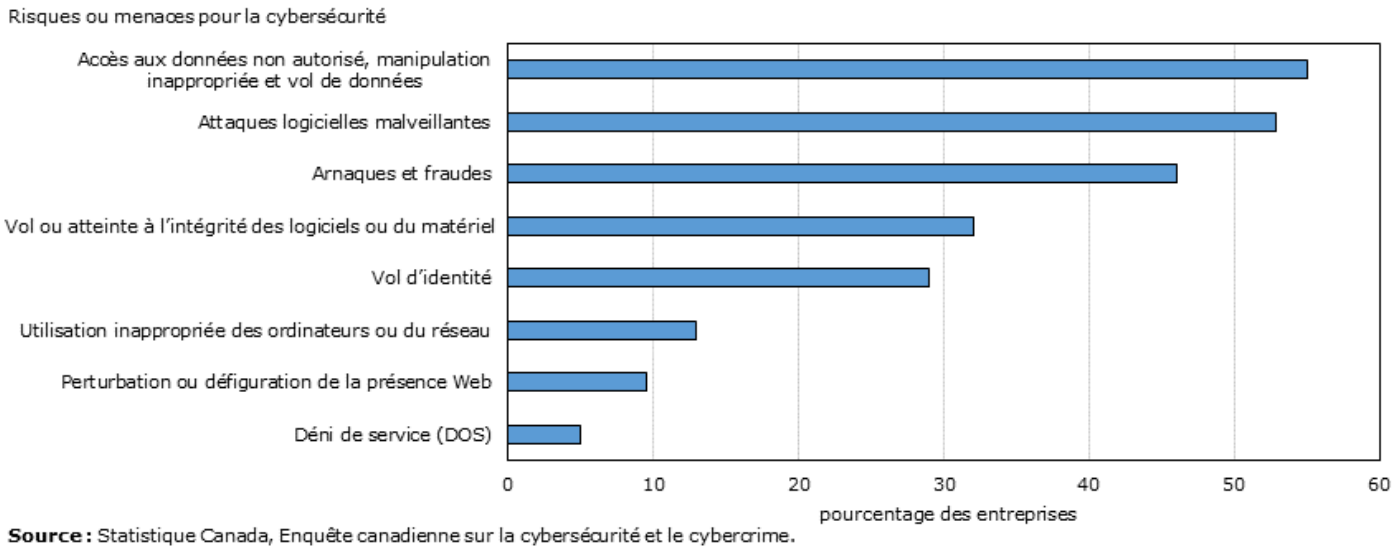
Parmi les entreprises touchées par des brèches de sécurité ou des attaques cybernétiques au Royaume-Uni et qui ont signalé leur brèche la plus perturbatrice à un tiers, 39 % ont signalé l'incident à un fournisseur de services de cybersécurité externes, 16 % l'ont signalé à un service de police, 11 % l'ont signalé à leur fournisseur de services Internet, et 10 % à une banque, à une association d'épargne immobilière ou à une société de cartes de crédit. Très peu (5 %) de ces entreprises ont signalé les incidents de cybersécurité dont elles ont été victimes à leurs clients, et encore moins (3 %) l'ont signalé à leurs fournisseurs.

Dans la plupart des cas (57 %), les incidents de cybersécurité qui ont touché les entreprises au Royaume-Uni ont été détectés par des membres du personnel de l'entreprise, des entrepreneurs ou des bénévoles. Cependant, environ 6 % des entreprises au Royaume-Uni ont été avisées d'un incident de cybersécurité par des clients.

La majorité des entreprises canadiennes sont préoccupées par leur vulnérabilité au cybercrime

Dans le cadre de l'ECCC de 2017, la majorité (85 %) des entreprises canadiennes ont déclaré être préoccupées par leur vulnérabilité aux futurs risques et menaces en matière de cybersécurité, et 8 % ont mentionné être extrêmement préoccupées. Parmi les entreprises qui se sont dites préoccupées par les futures menaces en matière de cybersécurité, 60 % ont affirmé que l'accès non autorisé aux données ainsi que la manipulation inappropriée et le vol de données entraîneraient des conséquences néfastes sur leurs activités. Plus de la moitié (56 %) des entreprises ont déclaré que les attaques provenant de logiciels malveillants (p. ex. virus, logiciels publicitaires ou logiciels de rançon) seraient dommageables pour leurs activités, et environ 47 % d'entre elles ont indiqué que les arnaques et la fraude (p. ex. fraude financière ou hameçonnage) entraîneraient des conséquences négatives sur leurs activités (graphique 4).

Graphique 4
Risques ou menaces liés à la cybersécurité qui seraient les plus nuisibles, Canada, 2017



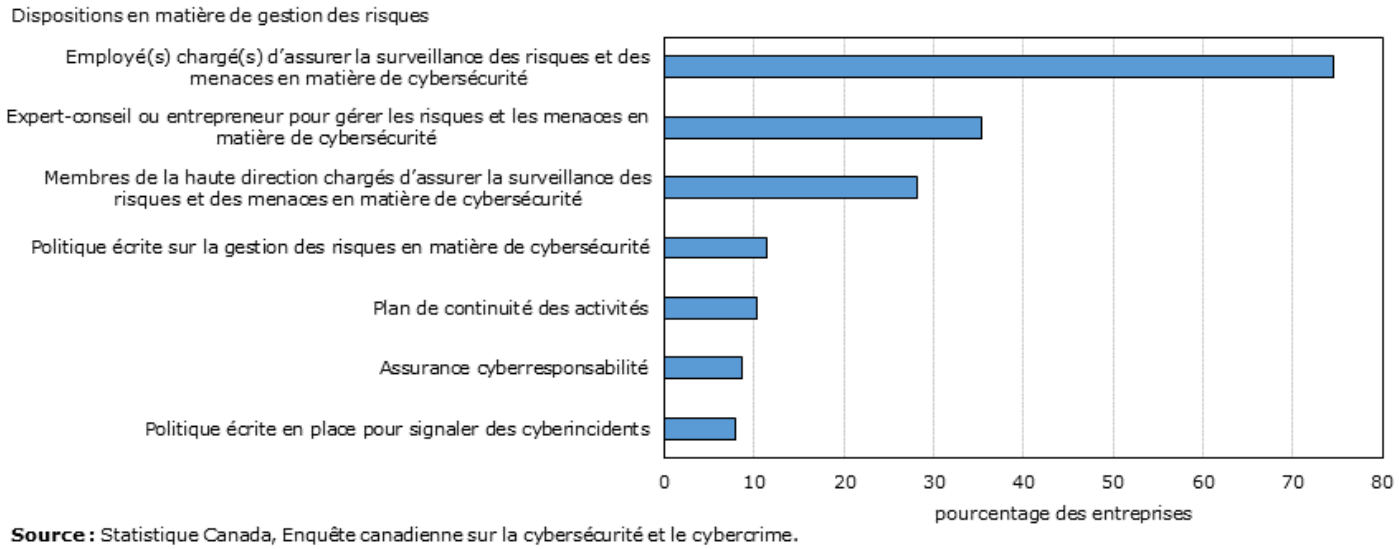
Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime.

Malgré ces préoccupations, seulement 28 % des entreprises ont déclaré que des membres de la haute direction étaient chargés d'assurer la surveillance des risques et des menaces en matière de cybersécurité. Le pourcentage d'entreprises dont les membres de la haute direction étaient chargés d'assurer la surveillance en matière de cybersécurité variait selon la taille, allant de 52 % pour les grandes entreprises à environ 26 % pour les petites entreprises.

En fait, cette mesure de gestion des risques était plus courante parmi les entreprises de certains secteurs, notamment les entreprises de conception de systèmes informatiques et de services connexes[17] (69 %), les entreprises de production, de transport et de distribution d'électricité (68 %) et les entreprises de traitement de données, d'hébergement de données et de services connexes[18] (67 %).

Plus de la moitié (58 %) des entreprises ont déclaré que les membres de la haute direction recevaient des mises à jour sur les mesures prises en matière de cybersécurité, mais très peu (6 %) d'entre elles avaient les outils leur permettant d'assurer le suivi des questions relatives à la cybersécurité. Le manque de participation de la haute direction est aussi attribuable au fait que les employés de la plupart (83 %) des entreprises n'informaient pas les membres de la haute direction des mesures prises en matière de cybersécurité après un incident de cybersécurité. Cela peut s'expliquer par le fait que très peu (8 %) d'entreprises avaient en place une politique écrite sur le signalement des incidents de cybersécurité. De plus, peu d'entreprises avaient en place une politique écrite sur la gestion des risques en matière de cybersécurité (11 %) ou un plan de continuité des activités en cas de détection de cybermenaces, de vulnérabilités et de risques (10 %) (graphique 5).

Graphique 5
Types de dispositions utilisés en matière de gestion des risques, Canada, 2017



Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime.

L'absence de politiques écrites et de participation de la haute direction présente un grave risque pour les entreprises canadiennes, car l'inadéquation des mesures visant à protéger la vie privée et les données augmente le risque de cybercrime. L'utilisation limitée de ces mesures de gestion des risques va également à l'encontre des recommandations formulées aux entreprises par le Centre canadien pour la cybersécurité, selon lesquelles la participation de la haute direction aux processus d'atténuation des risques est essentielle au renforcement des comportements appropriés des utilisateurs et à la réduction de la vulnérabilité au moyen de contrôles de sécurité adéquats (Centre canadien pour la cybersécurité, 2018).

Les entreprises canadiennes ont dépensé en moyenne 78 000 $ pour la prévention et la détection des incidents de cybersécurité

La grande majorité (94 %) des entreprises canadiennes ont engagé un certain niveau de dépenses pour mettre en place des mesures visant à prévenir et à détecter les incidents de cybersécurité en 2017. En moyenne, les entreprises canadiennes ont dépensé 78 000 $ à ces fins. Les grandes entreprises (dépenses moyennes de 922 000 $) sont celles qui ont engagé les dépenses les plus élevées, suivies des moyennes entreprises (dépenses moyennes de 108 000 $). Les petites entreprises ont déclaré avoir dépensé en moyenne 44 000 $.

Ce sont les entreprises du transport par pipeline qui ont dépensé le plus en moyenne (2,2 millions de dollars) pour des mesures de prévention et de détection des incidents de cybersécurité, suivies des entreprises de distribution de gaz naturel (1,2 million de dollars) et des établissements bancaires[8] (1,1 million de dollars).

Pour l'ensemble des entreprises, les dépenses moyennes totales consacrées aux salaires des employés chargés de la prévention et de la détection des incidents de cybersécurité se sont chiffrées à 40 000 $. Les entreprises ont également dépensé en moyenne 32 000 $ pour d'autres services professionnels, scientifiques et techniques, et 20 000 $ pour l'embauche d'experts-conseils ou d'entrepreneurs en TI en 2017[19].

Chez les grandes entreprises, les dépenses engagées pour mettre en place des mesures de prévention et de détection des incidents de cybersécurité étaient nettement différentes d'un volet à l'autre. Les dépenses moyennes engagées pour des services professionnels, scientifiques et techniques se sont chiffrées à 327 000 $, tandis que les dépenses moyennes totales consacrées aux salaires des employés chargés de la prévention et de la détection du cybercrime se sont établies à 305 000 $. Enfin, les dépenses moyennes engagées pour les services d'experts-conseils ou d'entrepreneurs en TI se sont élevées à 202 000 $.

Plus des deux tiers (68 %) des entreprises ont déclaré que l'une des raisons les ayant incitées à consacrer du temps ou de l'argent à la prévention du cybercrime était de protéger les renseignements personnels de leurs employés, leurs fournisseurs, leurs clients ou leurs partenaires. Environ 41 % ont affirmé que l'une de leurs principales raisons était d'empêcher la fraude et le vol, et environ 31 % ont mentionné que leurs dépenses étaient consacrées aux mesures de cybersécurité visant à assurer la continuité de leurs activités.

Encadré 3
Les entreprises au Royaume-Uni sont moins nombreuses à investir dans la cybersécurité que les entreprises canadiennes

Environ les deux tiers (66 %) des entreprises au Royaume-Uni consacraient un certain niveau de dépenses à la cybersécurité, tandis que cette proportion était beaucoup plus élevée au Canada. Comme au Canada, les dépenses engagées par les entreprises au Royaume-Uni étaient nettement plus élevées dans certains secteurs. Plus précisément, les entreprises du secteur de la finance et des assurances ont consacré en moyenne 30 000 $ à la cybersécurité, suivies des entreprises du secteur de l'information ou des communications, qui ont dépensé en moyenne 24 000 $, et de celles du secteur de l'éducation, qui ont dépensé en moyenne 14 000 $. Ces investissements étaient en grande partie motivés par des raisons semblables à celles des entreprises canadiennes.

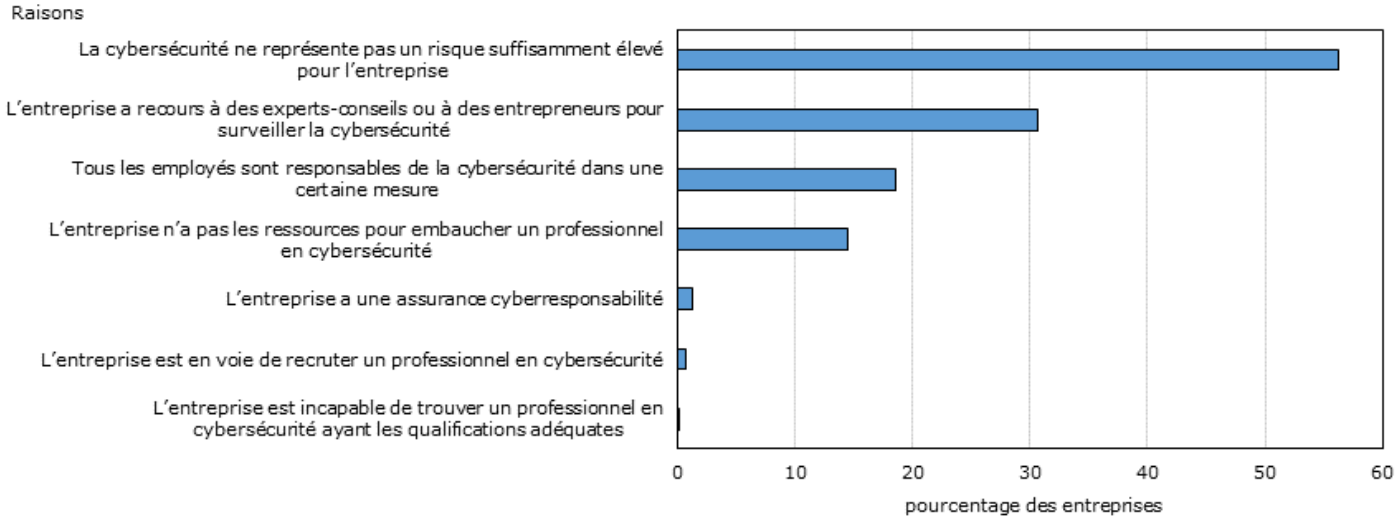
La majorité des entreprises canadiennes comptent des employés principalement responsables de la cybersécurité

La majorité des grandes (91 %), des moyennes (83 %) et des petites (72 %) entreprises au Canada ont déclaré avoir des employés principalement responsables de la cybersécurité générale de l'entreprise en 2017.

Les deux tiers (67 %) des entreprises, peu importe leur taille, ont affirmé compter au moins 1 à 5 employés principalement responsables de la cybersécurité. Le quart (24 %) des grandes entreprises ont déclaré compter plus de cinq employés principalement responsables de la cybersécurité, comparativement à 9 % des moyennes entreprises.

Parmi la proportion (26 %) d'entreprises qui ne comptaient pas d'employés principalement responsables de la cybersécurité, plus de la moitié (56 %) ont déclaré que la cybersécurité ne représentait pas un risque suffisamment élevé pour leur entreprise, et près du tiers (31 %) ont dit avoir plutôt eu recours à des experts-conseils ou à des entrepreneurs pour surveiller leur réseau. Il convient de noter que près de 19 % des entreprises ont déclaré que tous les employés étaient responsables de la cybersécurité dans une certaine mesure, et qu'environ 15 % ont expliqué que l'entreprise n'avait pas les ressources nécessaires pour embaucher un professionnel en cybersécurité (graphique 6).

Graphique 6
Principales raisons de ne pas avoir d'employés principalement responsables de la cybersécurité, Canada, 2017



Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime.

Un peu plus de la moitié (51 %) des entreprises ont informé leurs employés sur les pratiques générales en matière de cybersécurité au moyen de courriels, de babillards ou de séances d'information. Ces pratiques générales fournissaient souvent de l'information sur la façon de reconnaître et d'éviter les arnaques par courriel, l'importance de la complexité des mots de passe et les pratiques sécuritaires de navigation sur le Web.

Environ 19 % des entreprises ont offert une formation officielle à leurs employés pour perfectionner ou mettre à jour leurs compétences en cybersécurité. Cette formation a été offerte à une proportion presque égale de membres du personnel de la TI et d'autres employés de l'entreprise. Les grandes entreprises (59 %) étaient plus susceptibles d'offrir de la formation à leurs employés que les moyennes (32 %) et les petites entreprises (16 %). En moyenne, les entreprises canadiennes ont

dépensé 12 000 $ au cours de l'année pour offrir de la formation sur la cybersécurité à leurs employés, leurs fournisseurs, leurs clients ou leurs partenaires.

De plus, le recours à des experts-conseils ou à des entrepreneurs pour gérer les risques et les menaces liés à la cybersécurité était également très fréquent. Environ 45 % des moyennes entreprises ont eu recours à des services d'experts-conseils et d'entrepreneurs, comparativement à 38 % des grandes entreprises et à 33 % des petites entreprises. L'utilisation de ces services était couramment déclarée par les entreprises de services juridiques[20] (72 %).

Encadré 4
Les entreprises au Royaume-Uni étaient plus susceptibles de confier les responsabilités en matière de cybersécurité à des services externes

Les entreprises au Royaume-Uni étaient plus susceptibles de confier la gestion de leur cybersécurité à des services externes (49 %) que d'avoir du personnel affecté à la sécurité ou à la gouvernance de l'information (35 %). Comme les entreprises canadiennes, les moyennes entreprises (64 %) au Royaume-Uni étaient plus susceptibles d'avoir eu recours à des services externes pour leurs pratiques de gestion de la cybersécurité que les petites et grandes entreprises. Ce sont surtout les entreprises du secteur de la finance et des assurances (73 %) qui ont eu recours à des services externes.

De même, le fait d'avoir au moins un employé responsable de la cybersécurité était plus courant chez les grandes entreprises (76 %) que chez les moyennes (62 %) et petites (39 %) entreprises. Au Royaume-Uni, les entreprises qui étaient les moins susceptibles d'avoir des employés responsables de la cybersécurité relevaient des secteurs de la construction (22 %) et des services d'hébergement et de restauration (21 %). Au Canada, les entreprises les moins susceptibles de compter des employés responsables de la cybersécurité relevaient des sous-secteurs des magasins d'alimentation[21] (53 %) et des stations-service[22] (58 %) en 2017.

De plus, peu de différences ont été constatées entre les deux pays en ce qui concerne la formation en cybersécurité offerte au personnel. Au Royaume-Uni, environ 20 % des entreprises ont offert de la formation à leur personnel par l'entremise de programmes internes ou externes, comparativement à 19 % au Canada.

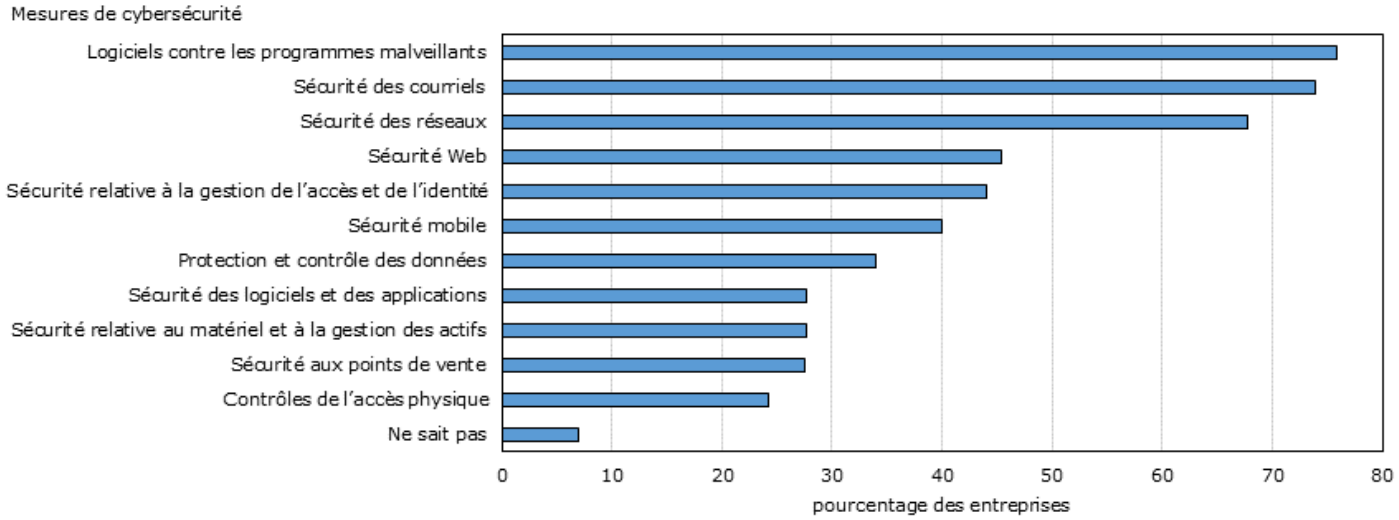
L'utilisation de mesures de cybersécurité s'est accrue depuis 2013, surtout en ce qui concerne les logiciels contre les programmes malveillants

En 2017, très peu (5 %) d'entreprises canadiennes ont déclaré ne pas avoir de mesures de cybersécurité en place pour se protéger ainsi que pour protéger leurs clients et leurs partenaires. Plus des trois quarts (76 %) ont déclaré avoir en place des logiciels contre les programmes malveillants pour se protéger des virus, des logiciels espions, des logiciels de rançon et d'autres attaques semblables, soit à peu près le même pourcentage d'entreprises qui ont déclaré utiliser de tels logiciels en 2013 (Statistique Canada, 2013c).

L'utilisation d'autres mesures de cybersécurité a toutefois considérablement augmenté. En 2017, la majorité des entreprises avaient en place des mesures pour assurer la sécurité des courriels (74 %) et des réseaux (68 %), tandis qu'en 2013, environ 53 % des entreprises avaient déclaré utiliser des filtres pourriels et 62 % avaient en place un pare-feu.

Près de la moitié (45 %) des entreprises utilisaient des mesures de sécurité Web, comme des restrictions aux sites Web, et 44 % avaient en place des mesures de gestion de l'accès et de l'identité en 2017. En comparaison, 13 % des entreprises utilisaient des logiciels de filtrage de contenu Web et 19 % utilisaient des logiciels ou du matériel d'authentification pour les utilisateurs internes ou externes en 2013 (Statistique Canada, 2013c) (graphique 7).

Graphique 7
Mesures de cybersécurité couramment utilisées, Canada, 2017



Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime.

Environ le tiers (29 %) des entreprises canadiennes ont été tenues, par leurs fournisseurs, leurs clients, leurs partenaires ou par des organismes de réglementation, de mettre en œuvre des mesures de cybersécurité en 2017. Ces exigences visaient plus couramment les établissements bancaires[8] (81 %), les magasins de produits de santé et de soins personnels[23] (79 %) et les entreprises du transport par pipeline (67 %).

Outre les mesures de cybersécurité déjà en place, plus de la moitié (58 %) des entreprises ont mis en œuvre des activités pour cerner les risques liés à la cybersécurité en 2017. La vaste majorité (93 %) des grandes entreprises ont mis en œuvre au moins une activité pour cerner les risques liés à la cybersécurité, comparativement à 78 % des moyennes entreprises et à 54 % des petites entreprises.

Les grandes entreprises étaient plus susceptibles de déclarer avoir eu recours à des services externes spécialisés pour évaluer leurs risques en matière de cybersécurité que les moyennes et les petites entreprises : 45 % ont embauché un tiers pour effectuer des tests d'intrusion visant à vérifier l'efficacité des dispositifs de sécurité, 37 % ont procédé à une vérification complète de leurs systèmes et 33 % ont eu recours à une évaluation officielle des risques liés à leurs pratiques en matière de cybersécurité.

Parmi les entreprises qui ont mis en œuvre des activités pour cerner les risques liés à la cybersécurité, la plupart (85 %) ont mené des activités de surveillance de leur réseau et de leurs systèmes internes, tandis que 38 % ont mené des activités de surveillance du comportement de leurs employés. Dans l'ensemble, ces types d'activités d'évaluation de la cybersécurité étaient plus courants chez les entreprises de production, de transport et de distribution d'électricité (97 %) et chez les établissements bancaires[8] (96 %).

Un peu plus de la moitié (52 %) des grandes entreprises menaient ces activités d'évaluation des risques selon un horaire précis. En revanche, 59 % des petites entreprises et 56 % des moyennes entreprises menaient ces activités de façon irrégulière.

En 2017, certaines entreprises canadiennes avaient également mis en place des mesures de sécurité supplémentaires : près du quart (24 %) des grandes entreprises ont déclaré avoir une assurance cyberresponsabilité pour se protéger contre les risques et les menaces liés à la cybersécurité, comparativement à 14 % des moyennes entreprises et à 7 % des petites entreprises. Cette assurance était plus couramment utilisée par les entreprises de distribution de gaz naturel (54 %), les entreprises de traitement de données, d'hébergement de données et de services connexes (50 %), ainsi que les établissements bancaires[8] (48 %). Les entreprises de ces secteurs pourraient être plus susceptibles de souscrire à une assurance cyberresponsabilité puisqu'elles sont considérées comme des cibles de grande valeur.

En moyenne, les entreprises canadiennes ont dépensé 14 000 $ au cours de l'année pour une assurance cyberresponsabilité. La majorité des polices d'assurance comprenaient une couverture contre les pertes directes découlant d'une attaque ou d'une intrusion (82 %), de l'interruption des activités (72 %), des frais de restauration (71 %) ainsi qu'une couverture contre les pertes liées à la responsabilité envers les tiers et contre les pertes financières (66 %).

Encadré 5
Les entreprises au Royaume-Uni sont plus nombreuses que les entreprises canadiennes à utiliser des logiciels contre les programmes malveillants, des mesures de sécurité des réseaux et des protocoles de gestion de l'accès et de l'identité

La grande majorité (92 %) des entreprises au Royaume-Uni ont déclaré avoir des règles ou des contrôles en place pour veiller à ce que les mises à jour logicielles soient effectuées lorsqu'elles étaient disponibles, et environ 90 % avaient une protection à jour contre les programmes malveillants. Comparativement aux entreprises canadiennes, un plus grand nombre d'entreprises au Royaume-Uni utilisaient également des mesures de sécurité des réseaux (89 % avaient un pare-feu) et des protocoles de gestion de l'accès et de l'identité (78 % restreignaient les droits et les accès d'administrateur de la TI à certains utilisateurs).

Environ le même pourcentage d'entreprises (38 %) au Canada et au Royaume-Uni surveillaient l'activité des utilisateurs, et environ 12 % des entreprises au Royaume-Uni exigeaient que leurs fournisseurs respectent des normes minimales de cybersécurité.

À l'instar des entreprises canadiennes, plus de la moitié (56 %) des entreprises au Royaume-Uni ont pris des mesures pour cerner les risques liés à la cybersécurité de leur organisation. La plupart (89 %) des grandes entreprises au Royaume-Uni ont mis en place une ou plusieurs mesures, comme confier l'évaluation officielle des risques ou la vérification de leurs systèmes à une partie interne ou externe.

Le taux d'entreprises ayant souscrit à une police d'assurance cyberresponsabilité était également semblable au Royaume-Uni et au Canada (9 %). Au Royaume-Uni, les grandes (24 %) et les moyennes (19 %) entreprises, de même que les entreprises du secteur de la finance et des assurances (20 %), étaient plus susceptibles d'avoir acheté une police d'assurance cyberresponsabilité.

Résumé

En 2017, un peu plus du cinquième (21 %) des entreprises canadiennes ont déclaré avoir été touchées par des incidents de cybersécurité qui ont eu des répercussions sur leurs activités. Parmi les entreprises qui ont pu déterminer le motif des attaques, 38 % ont été victimes d'une tentative de vol d'argent ou d'une demande de paiement d'une rançon. Plus du quart (26 %) des entreprises ont été victimes d'incidents où les auteurs ont tenté d'accéder à des zones d'accès non autorisé ou privilégié, tandis que 23 % ont été touchées par des incidents où il y a eu tentative de vol de renseignements personnels ou financiers.

Les entreprises de certains secteurs étaient plus susceptibles d'être touchées par des incidents de cybersécurité en 2017, notamment les établissements bancaires[8] (47 %), les universités (46 %) et les entreprises du transport par pipeline (45 %).

Plus du tiers (38 %) des entreprises n'ont signalé aucun incident de cybersécurité ayant eu des répercussions sur leurs activités à un tiers. Parmi les entreprises qui ont signalé des incidents de cybersécurité, environ 42 % l'ont signalé à leur expert-conseil ou à leur entrepreneur en TI, et 15 % l'ont signalé à leurs fournisseurs, à leurs clients ou à leurs partenaires. Peu d'entreprises (10 %) ont signalé des incidents de cybersécurité aux services de police en 2017.

En moyenne, les entreprises canadiennes ont dépensé 78 000 $ en 2017 pour prévenir et détecter les incidents de cybersécurité. Les grandes entreprises ont engagé les dépenses les plus élevées (dépenses moyennes de 922 000 $), suivies des moyennes entreprises (dépenses moyennes de 108 000 $). Les petites entreprises ont déclaré avoir dépensé en moyenne 44 000 $.

Très peu (5 %) d'entreprises canadiennes ont déclaré ne pas avoir de mesures de cybersécurité en place pour se protéger ainsi que pour protéger leurs clients et leurs partenaires en 2017. Environ 74 % des entreprises avaient des employés principalement responsables de la cybersécurité de leur entreprise, tandis que 31 % ont mentionné avoir uniquement recours à des experts-conseils ou à des entrepreneurs pour surveiller leur réseau.

Principaux termes et définitions clés

Appareils « intelligents » connectés à Internet : Appareils électroniques qui peuvent se brancher les uns aux autres et sur Internet au moyen d'un réseau. Ces appareils sont conçus pour envoyer et recevoir automatiquement des renseignements sur Internet de façon constante.

Chiffrement : Conversion d'information en un code que seuls les utilisateurs autorisés peuvent lire, c'est-à-dire ceux qui ont reçu la « clé » (habituellement unique) et le logiciel spécial qui leur permettront de renverser le processus (déchiffrement) et d'utiliser l'information.

Contrôle d'accès physique : Contrôle permettant aux utilisateurs autorisés d'accéder à un lieu ou à d'autres ressources (p. ex. tourniquets, cartes d'accès, mots de passe).

Déni de service : Cyberattaque par laquelle l'auteur tente de rendre les ressources d'une machine ou d'un réseau inaccessibles aux utilisateurs visés en perturbant temporairement ou indéfiniment les services d'un hôte connecté à Internet.

Filtre pourriel : Ensemble de règles permettant de filtrer les courriels qui ont été envoyés sans la permission ou la demande de l'utilisateur à qui ils ont été acheminés.

Fraude financière : Tentative d'un criminel d'obtenir, par des moyens frauduleux, le numéro de compte bancaire d'une victime, les renseignements d'ouverture de session de ses services bancaires en ligne et/ou ses renseignements de carte de crédit dans le but de voler de l'argent.

Gestion des droits : Restrictions visant la création et l'utilisation de contenu protégé, comme les courriels et les documents.

Hameçonnage : Type particulier de pourriel visant un ou plusieurs utilisateurs précis et que l'auteur tente de faire passer pour un message légitime en ayant l'intention de frauder le ou les destinataires.

Informatique en nuage : Capacité d'accéder à des logiciels, à des données et à des ressources par le réseau, au lieu d'y accéder de façon traditionnelle, soit par le biais des données sauvegardées localement sur l'ordinateur de l'utilisateur.

Logiciel contre les programmes malveillants : Type de logiciel conçu pour empêcher la contamination des dispositifs informatiques individuels et des systèmes de TI par des programmes malveillants, et pour détecter leur présence et remédier au problème.

Logiciel de filtrage de contenu Web : Logiciel qui empêche les utilisateurs d'accéder à certaines adresses Internet afin de protéger l'appareil et/ou le réseau informatique de l'utilisateur contre les attaques.

Logiciel de rançon : Type de logiciel malveillant qui restreint l'accès à l'ordinateur ou aux fichiers de l'utilisateur et qui affiche un message où l'on exige un paiement afin de retirer la restriction.

Logiciel espion : Logiciel qui recueille des renseignements sur un utilisateur à son insu. Il se présente souvent sous la forme d'un téléchargement « gratuit » et s'installe automatiquement avec ou sans consentement.

Logiciel ou matériel d'authentification : Logiciel ou matériel utilisé pour authentifier ou vérifier l'identité d'un utilisateur avant de lui accorder l'accès ou d'approuver une demande de transaction.

Logiciel publicitaire : Logiciel qui affiche ou qui télécharge automatiquement du matériel publicitaire (souvent non sollicité) lorsque l'utilisateur est en ligne.

Médias sociaux : Sites Web de réseautage social ou applications comme Facebook, Twitter et LinkedIn. Les entreprises s'en servent pour atteindre des clients potentiels, nouer des relations plus solides et à des fins de marketing ou à d'autres fins professionnelles.

Mesures de gestion de l'accès et de l'identité : Mesures mises en œuvre sur un réseau informatique pour gérer l'accès à des comptes d'utilisateur particuliers et assurer leur sécurité de façon continue (p. ex. règles de complexité des mots de passe, restrictions fondées sur les comptes d'utilisateur).

Pare-feu : Dispositif matériel et/ou logiciel, installé sur un ordinateur, qui contrôle l'accès entre un réseau privé et un réseau public, tel qu'Internet. Un pare-feu est conçu pour fournir une protection en interceptant un accès non autorisé à l'ordinateur ou au réseau.

Plan de continuité des activités : Stratégie permettant de reconnaître les menaces et les risques auxquels une entreprise fait face dans le but de s'assurer que les utilisateurs et les biens sont protégés, et que les tâches puissent continuer d'être effectuées en cas de problème majeur.

Plateforme de commerce électronique : Technologie logicielle qui permet à une entreprise de créer et d'héberger des vitrines virtuelles qui font appel à un ensemble de produits ou de services précis.

Sécurité de réseau : Protection de l'accès aux fichiers et aux répertoires d'un réseau informatique contre le piratage, l'utilisation malveillante et les changements non autorisés au système.

Sécurité des courriels : Toutes les mesures de sécurité utilisées pour filtrer et gérer les courriels qu'un utilisateur reçoit, et pour sécuriser l'accès à son compte (p. ex. filtres pourriels, analyses de courriels).

Sécurité du point de vente : Logiciel sécurisé permettant d'enregistrer les ventes de biens et services aux clients.

Sécurité mobile : Protection des téléphones intelligents, des tablettes, des ordinateurs portables et des autres appareils informatiques portables, ainsi que des réseaux auxquels ils sont connectés, contre les menaces et les vulnérabilités associées à l'informatique sans fil.

Sécurité Web : Domaine de la sécurité informatique lié précisément à Internet touchant la sécurité des utilisateurs, mais aussi la sécurité des réseaux de façon plus générale, car il s'applique à d'autres applications ou aux systèmes d'exploitation dans leur ensemble. L'objectif est d'établir des règles et des mesures pour se protéger contre les attaques perpétrées sur Internet.

Services Web : Services mis à la disposition des internautes ou d'autres programmes connectés à Internet à partir du serveur Web d'une entreprise. Des exemples courants de services Web pourraient être la gestion du stockage ou une application de gestion des relations avec les clients.

Stockage en nuage : Données stockées sur des serveurs Internet auxquels on peut accéder et que l'on peut partager à distance.

Temps d'arrêt : Période pendant laquelle une machine, un domaine ou un service n'est pas en fonction, par exemple, pendant des réparations, une défaillance ou des travaux d'entretien. Cette situation peut mener à une réduction de l'activité ou à l'inactivité d'un utilisateur ou d'une entreprise.

Test d'intrusion : Attaque simulée autorisée contre un système informatique dans le but de déceler les vulnérabilités qui pourraient permettre l'accès aux fonctions et aux données du système. Le test permet de déterminer si l'infrastructure de TI est vulnérable aux attaques et si les mécanismes de défense sont suffisants, ainsi que de déterminer quels mécanismes de défense ont été déjoués, le cas échéant.

Virus : Programme informatique malveillant qui est souvent envoyé sous forme de pièce jointe à un courriel ou par l'intermédiaire d'un téléchargement dans le but d'infecter un ordinateur ou un réseau. Il se présente souvent sous forme de pourriel et permet aux criminels d'accéder à votre ordinateur ou à votre réseau et de désactiver vos paramètres de sécurité.

Voix sur le protocole Internet : Acheminement de conversations vocales grâce à Internet. Il s'agit d'un processus différent d'un appel téléphonique, lequel est fait à partir du téléphone de la maison ou du bureau et qui passe par le réseau téléphonique commuté public.

Description de l'enquête

Enquête canadienne sur la cybersécurité et le cybercrime

L'Enquête canadienne sur la cybersécurité et le cybercrime (ECCC) a été menée pour la première fois en 2018 pour le compte de Sécurité publique Canada. Le but de l'enquête était de recueillir des données sur l'incidence du cybercrime sur les entreprises canadiennes ainsi que des données sur les activités menées en vue d'en atténuer les répercussions.

Cette enquête a été créée pour surveiller l'évolution rapide de l'environnement qui entoure la cybersécurité et le cybercrime, et pour établir des repères dans le domaine. Comme il s'agit d'un enjeu émergent, des données de ce type et de cette ampleur n'avaient jamais été recueillies auparavant par le gouvernement du Canada.

Les données de l'enquête ont été recueillies de janvier à avril 2018 au moyen d'un questionnaire électronique. La population cible comprenait les entreprises menant des activités au Canada et comptant au moins 10 employés, dans tous les secteurs, à l'exception du secteur des administrations publiques. Les entreprises menant des activités dans toute province ou tout territoire du Canada étaient visées par cette enquête.

Le questionnaire de l'enquête a été envoyé au gestionnaire de la TI de l'entreprise ou au cadre supérieur qui connaissait le mieux les pratiques de cybersécurité de l'entreprise. On a demandé aux répondants de fournir des renseignements sur les incidents de cybersécurité qui ont eu des répercussions sur les activités de l'entreprise en 2017. Le taux de réponse a été de 86 %, ce qui a produit un échantillon de 10 794 entreprises.

Limites des données

Étant donné que les entreprises ne sont pas toujours au courant des incidents de cybersécurité qui les touchent ou qu'elles ne sont pas disposées à signaler certains incidents, les résultats de l'enquête peuvent avoir fait l'objet d'un biais de sous-déclaration.

Dans le cadre de l'ECCC, on a seulement demandé aux entreprises de déclarer les incidents qui ont eu des répercussions sur leurs activités. Par conséquent, les incidents que les entreprises ont jugés sans effet ne sont pas saisis dans ces données.

Enquête sur les brèches de cybersécurité de 2018 au Royaume-Uni

L'enquête sur les brèches de cybersécurité au Royaume-Uni, menée en 2018 par le ministère du Numérique, de la Culture, des Médias et des Sports du Royaume-Uni, fournit des renseignements sur les comportements et les pratiques des entreprises et des organismes caritatifs du Royaume-Uni en réponse aux menaces à la cybersécurité. L'enquête était divisée en deux parties, la première étant une enquête probabiliste aléatoire menée par téléphone auprès de 1 519 entreprises et de 569 organismes caritatifs enregistrés du Royaume-Uni. Cette partie de l'enquête s'est déroulée du 9 octobre au 14 décembre 2017. La deuxième partie était une interview de suivi menée auprès de 50 répondants ayant participé à la première partie de l'enquête, ainsi qu'auprès d'établissements d'enseignement supérieur. Cette partie de l'enquête a eu lieu en janvier et février 2018.

Aux fins du présent article, l'information tirée de la première partie de l'enquête réalisée au Royaume-Uni a été comparée aux résultats de l'ECCC, lorsqu'il y avait lieu. Cette comparaison a été effectuée avec les résultats de l'enquête menée au Royaume-Uni sur les entreprises uniquement, puisque les organismes caritatifs étaient hors du champ de l'ECCC. L'analyse des deux ensembles de données n'a pas fait l'objet d'une estimation de la variance ni d'un test d'hypothèse. Pour de plus amples renseignements sur la méthodologie et la stratégie d'échantillonnage de l'enquête réalisée au Royaume-Uni, veuillez consulter le document du ministère du Numérique, de la Culture, des Médias et des Sports, 2018.

Références

BANQUE DU CANADA. 2017. « Taux de change annuels », *Banque du Canada*, 29 décembre (site consulté le 11 décembre 2018).

BIGO, Didier, et autres. 2012. *Fighting Cyber Crime and Protecting Privacy in the Cloud*, European Parliament Committee on Civil Liberties, Justice and Home Affairs, PE nº 462.509.

CENTRE CANADIEN DE CYBERSÉCURITÉ. 2018. *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information*, ITSM nº 10.189 (site consulté le 28 décembre 2018).

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. 2018. *De nouvelles obligations en matière de déclaration des atteintes aux données entrent en vigueur cette semaine*, communiqué du Commissariat à la protection de la vie privée du Canada (site consulté le 30 novembre 2018).

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE et COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ALBERTA. 2015. *Un programme « Apportez votre propre appareil » constitue-t-il le bon choix pour votre organisation?*, Commissariat à la protection de la vie privée du Canada (site consulté le 21 décembre 2018).

GENDRON, Angela, et Martin RUDNER. 2012. *Évaluation des cybermenaces pesant contre les infrastructures du Canada*, rapport préparé pour le Service canadien du renseignement de sécurité (site consulté le 28 décembre 2018).

MINISTÈRE DU NUMÉRIQUE, DE LA CULTURE, DES MÉDIAS ET DES SPORTS. 2018. Enquête sur les brèches de cybersécurité de 2018 [collecte de données], service de données du Royaume-Uni, nº d'enregistrement 8406.

SÉCURITÉ PUBLIQUE CANADA. 2009. *Stratégie nationale sur les infrastructures essentielles*, ISBN nº 978-1-100-90318-7 (site consulté le 27 décembre 2018).

STATISTIQUE CANADA. 2018a. *Programme de déclaration uniforme de la criminalité*, Enquêtes et programmes statistiques, Centre canadien de la statistique juridique, nº d'enregistrement 3302 (site consulté le 12 décembre 2018).

STATISTIQUE CANADA. 2018b. *Enquête sociale générale : l'aperçu*, Enquêtes et programmes statistiques, produit nº 89F0115X au catalogue de Statistique Canada (site consulté le 12 décembre 2018).

STATISTIQUE CANADA. 2013a. *Entreprises possédant un site Web selon l'industrie et la taille de l'entreprise*, tableau 22-10-0016-01 (site consulté le 28 novembre 2018).

STATISTIQUE CANADA. 2013b. *Fonction du site Web selon l'industrie et la taille de l'entreprise*, tableau 22-10-0017-01 (site consulté le 28 novembre 2018).

STATISTIQUE CANADA. 2013c. *Entreprises ayant déclaré des pratiques en matière de sécurité des technologies de l'information et des communications (TIC), selon l'industrie et la taille de l'entreprise*, tableau 22-10-0032-01 (site consulté le 28 novembre 2018).

VAN DER MEER, Sico. 2015. « Enhancing international cyber security », *Security & Human Rights*, vol. 26, nos 2 à 4, p. 193 à 205.

Notes

1. Statistique Canada recueille également des données sur le cybercrime au moyen du Programme de déclaration uniforme de la criminalité. Il s'agit d'une enquête annuelle sur les crimes déclarés par la police qui a été modifiée en 2004 afin de permettre aux services de police d'indiquer toute affaire de cybercriminalité, c'est-à-dire toute infraction relevant du *Code criminel* du Canada dans laquelle la technologie de l'information et des communications (TIC) est l'objet du crime, ou dans laquelle la TIC est nécessaire à la perpétration de l'infraction et en fait partie intégrante.

De plus, dans le cadre de la déclaration annuelle des statistiques sur la criminalité, Statistique Canada fait état de crimes qui sont intrinsèquement cybernétiques, tels que la distribution non consensuelle d'images intimes, le leurre d'enfants au moyen d'un ordinateur et la pornographie juvénile. Voir Statistique Canada, 2018a pour de plus amples renseignements.

Les données sur les enjeux sociaux qui sont souvent associés au cybercrime, comme la cyberintimidation et le cyberharcèlement, sont recueillies au moyen du module sur la victimisation de l'Enquête sociale générale (ESG). « Les données de l'ESG sont un complément important des données administratives sur les crimes déclarés par la police, parce qu'elles saisissent de l'information qui n'est pas signalée à la police et qui n'est donc pas prise en compte dans les taux de criminalité officiels. » (Statistique Canada, 2018b).

2. Aux fins de l'analyse des entreprises canadiennes selon leur taille, la population est répartie en petites entreprises (10 à 49 employés), en moyennes entreprises (50 à 249 employés) et en grandes entreprises (250 employés ou plus).

3. Les données sur l'utilisation des médias sociaux de 2017 ne sont pas directement comparables avec celles de 2013, puisque dans l'Enquête canadienne sur la cybersécurité et le cybercrime (ECCC) de 2017, on demandait aux répondants s'ils avaient un compte de médias sociaux, tandis que dans l'Enquête sur la technologie numérique et l'utilisation d'Internet (ETNUI) de 2013, on demandait aux répondants ayant un site Web s'ils avaient relié celui-ci à leurs comptes de médias sociaux.

Plus important encore, les données de 2013 de l'ETNUI comprennent les entreprises qui comptaient 0 employé ou plus, tandis que l'ECCC a été menée auprès des entreprises comptant 10 employés ou plus. Par conséquent, en raison de la divergence des méthodologies entre les enquêtes, il faut faire preuve de prudence au moment d'effectuer des comparaisons entre les données de ces deux enquêtes.

4. Code 211 du Système de classification des industries de l'Amérique du Nord (Extraction de pétrole et de gaz).

5. Code 622 du Système de classification des industries de l'Amérique du Nord (Hôpitaux).

6. Code 519 du Système de classification des industries de l'Amérique du Nord (Autres services d'information).

7. Code 2212 du Système de classification des industries de l'Amérique du Nord (Distribution de gaz naturel).

8. Codes 521 et 522 du Système de classification des industries de l'Amérique du Nord (Autorités monétaires — banque centrale et Intermédiation financière et activités connexes). Les services bancaires d'investissement en sont exclus.

9. Dans le cadre de l'Enquête canadienne sur la cybersécurité et le cybercrime, on a demandé aux répondants de signaler les types d'incidents qui ont eu des répercussions sur leurs activités. Les répondants ont aussi pu définir la nature des

incidents qui ont eu des répercussions sur leurs activités. Les données sur les incidents que les répondants ont évalués comme n'ayant eu aucune répercussion sur leurs activités n'ont pas été recueillies.

10. Code 6113 du Système de classification des industries de l'Amérique du Nord (Universités).

11. Code 486 du Système de classification des industries de l'Amérique du Nord (Transport par pipeline).

12. Parmi l'ensemble des entreprises au Royaume-Uni, le pourcentage d'entreprises touchées par des incidents de cybersécurité a été calculé à partir des microdonnées tirées de l'enquête sur les brèches de cybersécurité de 2018 menée au Royaume-Uni. Le calcul a été limité aux entreprises qui ont été victimes de brèches ou d'attaques de cybersécurité qui ont eu des répercussions sur leurs activités. Cette façon de procéder a permis de comparer les résultats de l'enquête du Royaume-Uni à ceux de l'Enquête canadienne sur la cybersécurité et le cybercrime. Cette valeur diffère de celle du communiqué statistique du Royaume-Uni, lequel a déclaré que 43 % des entreprises au Royaume-Uni avaient été victimes de brèches ou d'attaques de cybersécurité. La valeur présentée dans le communiqué statistique du Royaume-Uni comprenait les entreprises qui ont été victimes d'une attaque ou d'une brèche n'ayant pas eu de répercussions sur leurs activités.

13. La population d'entreprises au Royaume-Uni a été ventilée selon leur taille, soit les microentreprises (1 à 9 employés), les petites entreprises (10 à 49 employés), les moyennes entreprises (50 à 249 employés) et les grandes entreprises (250 employés ou plus).

14. Ces données ne sont pas directement comparables, puisque l'enquête sur les brèches de cybersécurité de 2018 menée au Royaume-Uni a permis de mesurer le temps nécessaire aux entreprises pour reprendre leurs activités à la suite d'un incident de cybersécurité, tandis que l'Enquête canadienne sur la cybersécurité et le cybercrime a permis de mesurer le temps d'arrêt des activités des entreprises à la suite d'un incident de cybersécurité.

15. Le calcul des coûts moyens de rétablissement des entreprises au Royaume-Uni comprend les valeurs « 0 », tandis que les coûts déclarés pour les entreprises canadiennes excluent ces valeurs. Par conséquent, il faut faire preuve de prudence au moment d'effectuer des comparaisons entre les coûts de rétablissement des deux pays.

Tous les coûts déclarés dans le cadre de l'enquête sur les brèches de cybersécurité de 2018 au Royaume-Uni ont été indiqués en livres sterling. Pour faciliter la comparaison, les coûts ont été convertis en dollars canadiens en utilisant le taux de change annuel moyen de 2017 publié par la Banque du Canada. Le taux de change était de 1,6720, exprimé en une unité de la livre sterling du Royaume-Uni convertie en dollars canadiens.

16. Code 2211 du Système de classification des industries de l'Amérique du Nord (Production, transport et distribution d'électricité).

17. Code 5415 du Système de classification des industries de l'Amérique du Nord (Conception de systèmes informatiques et services connexes).

18. Code 518 du Système de classification des industries de l'Amérique du Nord (Traitement de données, hébergement de données et services connexes).

19. Les valeurs « 0 » ont été exclues de tous les calculs en dollars des dépenses des entreprises canadiennes. Ainsi, les chiffres en dollars déclarés pour chaque volet de dépenses des entreprises canadiennes sont fondés sur des populations légèrement différentes; par conséquent, leur somme n'équivaut pas aux dépenses moyennes totales des entreprises.

20. Code 5411 du Système de classification des industries de l'Amérique du Nord (Services juridiques).

21. Code 445 du Système de classification des industries de l'Amérique du Nord (Magasins d'alimentation).

22. Code 447 du Système de classification des industries de l'Amérique du Nord (Stations-service).

23. Code 446 du Système de classification des industries de l'Amérique du Nord (Magasins de produits de santé et de soins personnels).