Profil des entreprises canadiennes qui signalent les cybercrimes à la police

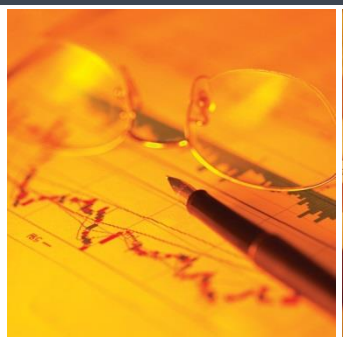
L'Enquête canadienne sur la cybersécurité et le cybercrime de 2017

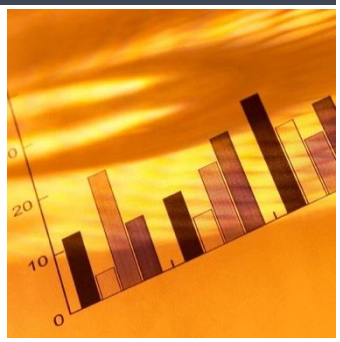
par Kayla A. Wanamaker

RAPPORT DE RECHERCHE : 2019–R006

DIVISION DE LA RECHERCHE

www.securitepublique.gc.ca





BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

Sécurité publique Canada | Public Safety Canada

Canada

Sommaire

Le cybercrime – à savoir les crimes commis à l'aide d'Internet et des technologies de l'information (TI), comme le piratage informatique, la propagation de virus et le crime organisé – préoccupe de plus en plus les gouvernements, organisations, individus et entreprises partout dans le monde. La recherche menée aux États-Unis, au Royaume-Uni et au Canada révèle que les incidents de cybercrime et de cybersécurité sont sous-signalés à la police, mais on en sait peu sur les raisons pourquoi il en est ainsi, surtout dans un contexte canadien. La présente étude avait donc pour but d'examiner le phénomène du sous-signalement des incidents de cybersécurité à la police, et ce à partir des données de l'Enquête canadienne sur la cybersécurité et le cybercrime de 2017, réalisée auprès d'entreprises canadiennes. Les résultats de l'Enquête indiquent que tout juste plus de 20 % des entreprises avaient été victimes de cyberincidents, mais seulement 10 % environ signalaient ces incidents à la police. Les entreprises ont dit ne pas avoir signalé les incidents parce que ceux-ci avaient été résolus à l'interne ou par l'intermédiaire d'un consultant en TI, ou parce qu'elles les avaient jugés trop mineurs pour les signaler à la police. Par ailleurs, l'Enquête a permis de constater que la gestion des risques, la formation officielle et la communication des pratiques exemplaires étaient liées à la probabilité de signaler les incidents à la police. Elle a également révélé que les grandes entreprises étaient plus susceptibles de signaler les cybercrimes à la police lorsqu'elles mettaient en œuvre un moins grand nombre de mesures de sécurité, alors que dans le cas des petites entreprises, les scores aux mesures de sécurité n'avaient rien à voir avec le signalement à la police. Enfin, les résultats de l'Enquête laissent entrevoir la nécessité d'accroître la sensibilisation à la fréquence des cybercrimes ainsi que d'offrir davantage d'options de formation officielle sur les cyberincidents, et soulignent l'importance d'améliorer les protocoles de cybersécurité.

Note de l'auteur

Les opinions exprimées dans le présent document sont celles des auteurs et ne traduisent pas nécessairement celles de Sécurité publique Canada. Prière d'acheminer toute correspondance à propos du présent rapport à l'adresse suivante :

Division de la recherche
Sécurité publique Canada
340, avenue Laurier Ouest
Ottawa (Ontario) K1A 0P8
Courriel : PS.CSCCBResearch-RechercheSSCRC.SP@canada.ca

Remerciements

L'auteure tient à remercier la Division des investissements, de la science et de la technologie de Statistique Canada d'avoir mené l'Enquête canadienne sur la cybersécurité et le cybercrime et apporté son soutien. Elle souhaite également remercier la Direction générale de la cybersécurité nationale de Sécurité publique Canada de son appui et de ses conseils continus en matière de cybersécurité et de cybercrime.

Renseignements sur le produit

Nº PS18-51/2019F-PDF
ISBN 978-0-660-33577-3

Table des matières

Introduction

Le cybercrime – qui comprend le piratage informatique, la propagation de virus et le crime organisé commis au moyen d'un ordinateur – préoccupe de plus en plus les gouvernements, organisations, individus et entreprises partout dans le monde (Kshetri, 2010), et a diverses répercussions économiques et sociales sur les entreprises (Kaplan, Sharma et Weinberg, 2011). En effet, étant donné l'utilisation répandue de la technologie et la numérisation des activités économiques, les entreprises se préoccupent de plus en plus de la sécurité de leurs systèmes et de leur réseau (Kaplan et al., 2011; Kshetri, 2010). Selon un rapport sur les risques liés à la cybersécurité produit par AON (2019), une connectivité accrue engendre des vulnérabilités nouvelles et amplifiées sur le plan de la sécurité. C'est pourquoi les entreprises craignent maintenant davantage d'être victimes de crimes cybernétiques que de crimes physiques (Keizer, 2006).

Une étude de recherche menée par McAfee (2018)[1] montre l'impact financier important du cybercrime, soit près de 600 milliards de dollars américains à l'échelle mondiale. Ce chiffre peut s'expliquer en partie par le fait que le cybercrime est devenu chose courante, près des deux tiers des gens qui utilisent des services en ligne en ayant été victimes sous une forme ou sous une autre. De plus, il arrive souvent que les auteurs de cybercrimes ne soient pas poursuivis en justice ou ne se fassent même pas prendre (McAfee, 2018).

Jusqu'à présent, la plupart des recherches examinant l'impact du cybercrime a été effectuée aux États-Unis (p. ex., Norton, 2018). Par conséquent, on ignore exactement à quel point le cybercrime est répandu au Canada – surtout parce que les organisations ne sont pas tenues de signaler les atteintes à la protection des données (Soloman, 2018) –, quoiqu'il émerge des recherches sur le sujet (p. ex., Statistique Canada, 2018a).

De très nombreux travaux de recherche ont permis de conclure que les cyberinfractions sont sous-signalées (Department for Digital, Culture, Media and Sport, 2018; Kethineni et Cao, 2019; Rantala, 2008; Statistique Canada, 2018a; Sukhai, 2004). Selon ces recherches, les entreprises s'abstiennent de signaler les crimes pour plusieurs raisons, notamment la croyance que l'incident n'est pas assez grave; la crainte de mauvaise publicité, ce qui minerait la confiance du public (Soloman, 2016; Sukhai, 2004) et nuirait à la crédibilité de l'entreprise (Kshetri, 2010); les perturbations découlant d'une enquête potentielle (Sukhai, 2004); et l'absence de garantie d'une indemnisation (Khalid, 2004).

Bien que maintes raisons puissent expliquer pourquoi les cybercrimes ne sont généralement pas signalés, il est essentiel de comprendre les raisons précises pourquoi certaines entreprises canadiennes ne signalent pas les cybercrimes, de même que les facteurs qui peuvent accroître la probabilité qu'un cyberincident soit signalé et les profils des entreprises qui signalent les cyberincidents. En effet, s'ils comprennent mieux quelles entreprises effectuent des signalements et ce qui les incite à le faire, les décideurs en matière de cybercrime et de sécurité nationale ainsi que les organismes d'application de la loi seront mieux outillés pour s'attaquer aux enjeux entourant le sous-signalement. C'est pourquoi la présente étude prend appui sur les données de

[1] En partenariat avec le Center for Strategic and International Studies.

l'Enquête canadienne sur la cybersécurité et le cybercrime de 2017 (ECCSCC), la première en son genre au Canada. Celle-ci a été réalisée auprès d'entreprises canadiennes en 2018 dans le but de cerner le nombre et le pourcentage d'entreprises qui signalent les cybercrimes aux autorités, les raisons pourquoi les cybercrimes ne sont pas signalés, ainsi que les caractéristiques des entreprises qui signalent les cybercrimes comparativement à celles qui ne le font pas, et ce afin qu'il soit possible de faire des prédictions.

Méthode

Enquête canadienne sur la cybersécurité et le cybercrime

L'ECCSCC de 2017 a été réalisée au nom de Sécurité publique Canada (SP) en partenariat avec Statistique Canada. Les données ont été collectées de janvier à avril 2018. Le but consistait à recueillir les données d'entreprises canadiennes sur les mesures de cybersécurité, les expériences du cybercrime et les activités en vue d'atténuer les effets du cybercrime sur les petites, moyennes et grandes entreprises. L'Enquête comptait 35 questions mesurant plusieurs aspects clés tels que les caractéristiques de l'entreprise, l'environnement de cybersécurité (p. ex., les mesures de sécurité actuellement en place), l'état de préparation en matière de cybersécurité (p. ex., les dispositions de gestion des risques actuellement en place), la résilience de l'entreprise (p. ex., les risques ou les menaces pour la cybersécurité qui sont considérés comme les plus préjudiciables à une entreprise), le coût de la prévention ou de la détection des incidents de cybersécurité, l'information au sujet des incidents de cybersécurité (p. ex., l'impact des incidents de cybersécurité sur les entreprises), le signalement des incidents de cybersécurité et le coût du rétablissement par suite d'un incident de cybersécurité. Pour en savoir davantage sur les résultats de l'Enquête, voir Statistique Canada (2018a). Il importe de noter que les données de l'Enquête sont les premières en leur genre à être recueillies au Canada, et c'est pourquoi elles serviront de jalon pour les futures enquêtes et stratégies de collecte de données.

Élaboration du questionnaire et mise à l'essai

L'ECCSCC a été conçue par Statistique Canada en consultation avec divers organismes gouvernementaux dont SP ainsi que des services de police, des experts en la matière, des universitaires, des entreprises privées et des associations de gens d'affaires. Après la création du questionnaire initial, deux rondes d'essai ont eu lieu, où on a demandé à 48 entreprises de Montréal, d'Ottawa, de Toronto et de Vancouver choisies au hasard de cerner tout enjeu lié au contenu et à l'enchaînement des questions. On a aussi tenu des réunions avec les gestionnaires des TI afin d'évaluer l'information recueillie et le langage employé dans le questionnaire. Dans l'ensemble, on a peaufiné le questionnaire jusqu'à obtenir les 35 questions utilisées pour la présente étude (Statistique Canada, 2018b). Le questionnaire devait prendre 30 minutes à remplir et portait sur les incidents de sécurité survenus au cours de l'année précédente (de janvier à décembre 2017).

Échantillon de l'Enquête

L'Enquête a été réalisée en ligne, et les données ont été collectées auprès d'entreprises menant des activités au Canada qui comptaient au moins dix employés, dans tous les secteurs sauf la fonction et l'administration publiques. Les entreprises dont les recettes se chiffraient à moins de

100 000 $ (ou 250 000 $ dans certains cas, selon le secteur) ont été exclues. Le questionnaire a été envoyé soit à la direction des TI, soit au membre chevronné du personnel connaissant le mieux les pratiques de cybersécurité de l'entreprise. Au total, 12 597 entreprises ont été incluses dans l'échantillon, sur une population de 194 569 entreprises partout au Canada; le taux de réponse était de 86 %, ce qui correspond à une taille d'échantillon finale de 10 794 entreprises. Quelque 44,9 % des répondants étaient des petites entreprises, 35,5 % des moyennes entreprises et 19,6 % des grandes entreprises[2]. Il importe de noter que les réponses ont été pondérées d'après le nombre d'entreprises d'une taille particulière (selon le nombre d'employés) composant la population. Ainsi, comme l'économie compte plus de petites entreprises, ce sont elles qui avaient le plus de poids.

Analyse des données

Diverses questions de l'Enquête portant sur le signalement des incidents à la police ont permis d'examiner la fréquence pour les diverses tailles d'entreprise – et en général (voir le tableau 1A à l'annexe A). Cet examen a été suivi d'une analyse de la variance visant à déterminer s'il y avait des différences en ce qui concerne les raisons de ne pas signaler les cyberincidents selon la taille de l'entreprise (voir le tableau 2A à l'annexe A). Par ailleurs, des moyennes, des écarts-types et des tests t ont servi à comparer les entreprises qui signalaient les cyberincidents à la police avec celles qui ne le faisaient pas (voir le tableau 3A à l'annexe A).

Enfin, pour déterminer si les entreprises qui signalent les incidents de cybersécurité à la police présentent des caractéristiques distinctes, et si certains facteurs sont associés aux raisons pourquoi les entreprises signalent ou non les cybercrimes à la police, on a réalisé des analyses de régression logistique pour les différentes tailles d'entreprise (voir le tableau 4A à l'annexe A). Pour être plus précis, on a examiné la taille de l'entreprise en tant que variable modératrice (où on a comparé les petites entreprises aux moyennes et grandes entreprises), afin de déterminer si certains facteurs prédisaient davantage le signalement des cyberincidents à la police chez les petites entreprises par rapport aux grandes entreprises, et vice versa. On a inclus dans les analyses de régression quatre prédicteurs qu'on a créés en additionnant les réponses oui/non tirées d'un sous-ensemble de questions de l'Enquête :

- *Protocoles de gestion des risques.* Les scores à la variable des protocoles de gestion des risques varient entre 0 et 7, où les scores élevés indiquent que l'entreprise a mis en place un plus grand nombre de protocoles de gestion des risques. Cette variable se compose de 7 questions fermées (L'entreprise a-t-elle une politique écrite? L'entreprise a-t-elle un plan de continuité?). La fiabilité a été jugée adéquate ($\alpha = 0,68$).
- *Formation officielle offerte par les entreprises.* Les scores à la variable de la formation officielle varient entre 0 et 3, où les scores élevés indiquent que l'entreprise a mis en place un plus grand nombre de mécanismes de formation officielle. Cette variable se compose de 3 questions fermées (L'entreprise assure-t-elle une formation à l'équipe interne des TI? Aux autres employés? Aux intervenants?). La fiabilité a été jugée adéquate ($\alpha = 0,69$).

[2] Les entreprises étaient considérées comme petites si elles comptaient de 10 à 49 employés, moyennes si elles comptaient de 50 à 249 employés, et grandes si elles comptaient 250 employés ou plus.

- *Mesures de cybersécurité mises en place.* Les scores à la variable des mesures de cybersécurité varient entre 0 et 11, où les scores élevés indiquent que l'entreprise a mis en place un plus grand nombre de mesures de sécurité. Cette variable se compose de 11 questions fermées (L'entreprise dispose-t-elle de mesures de sécurité des appareils mobiles? De mesure de sécurité du réseau? L'entreprise dispose-t-elle de mesures de gestion de l'identité?). La fiabilité a été jugée très bonne ($\alpha = 0{,}87$).
- *Communication des pratiques exemplaires aux employés et au personnel des TI.* Les scores à la variable de la communication des pratiques exemplaires varient entre 0 et 2, où les scores élevés indiquent que les pratiques exemplaires sont communiquées aux employés. Cette variable se compose de 2 questions fermées (L'entreprise communique-t-elle les pratiques exemplaires à ses employés?). Il n'a pas été possible d'évaluer la fiabilité de cette variable puisqu'elle se base sur deux questions seulement.

Résultats

Les résultats sont décrits dans deux sections principales; la première section présente les réponses à diverses questions de l'Enquête qui revêtent un intérêt particulier pour le présent rapport (dont la fréquence de signalement des cyberincidents à la police, les raisons pourquoi les entreprises n'ont pas signalé les incidents à la police et les types d'incident le plus souvent signalés à la police). Cette section se penche en outre sur les différences et les ressemblances entre les entreprises de différentes tailles au chapitre des réponses à l'Enquête. Pour sa part, la deuxième section donne les résultats des analyses de régression logistique, en précisant les variables les plus susceptibles de prédire le signalement des incidents à la police.

Analyses descriptives et différences selon la taille de l'entreprise

Le cinquième des entreprises sont victimes d'un cyberincident

Environ 20,8 % des entreprises avaient été victimes d'un cyberincident quelconque, soit 18,8 % des petites entreprises, 28,0 % des moyennes entreprises et 41,0 % des grandes entreprises (voir le tableau 1A à l'annexe A).

Moins de dix pour cent des entreprises signalent les cyberincidents à la police

Seulement 9,6 % des entreprises avaient signalé les incidents à la police, soit 8,4 % des petites entreprises, 12,5 % des moyennes entreprises et 15,0 % des grandes entreprises. Dans l'ensemble, seulement 6,3 % des entreprises avaient signalé tous les incidents de cybersécurité à la police (petites = 6,3%; moyennes = 6,2 %; grandes = 7,6 %) (voir le tableau 1A à l'annexe A).

Les cyberincidents signalés à la police concernent le vol de renseignements personnels ou financiers

Les signalements d'incidents de cybersécurité les plus couramment reçus par la police (d'après les données de l'Enquête) étaient les mêmes pour les petites, moyennes et grandes entreprises, et concernaient principalement le vol d'argent ou une demande de rançon (26,5 % des entreprises),

le vol de renseignements personnels ou financiers (17,4 % des entreprises) ou l'accès à des zones interdites (15,6 % des entreprises), ou encore des incidents commis pour une raison inconnue (9,5 % des entreprises).

Plus de la moitié des entreprises résolvent les cyberincidents à l'interne au lieu de les signaler à la police

Il importe de noter que les entreprises n'avaient pas signalé les incidents à la police pour les raisons suivantes : les incidents avaient été résolus à l'interne (52,1 %); les incidents avaient été résolus par l'intermédiaire d'un consultant en TI (32,5 %); les incidents étaient jugés trop mineurs pour être signalés à la police (29,1 %); l'entreprise n'avait pas pensé à communiquer avec la police (23,5 %); l'entreprise croyait que la police ne considérerait pas l'incident comme assez important (18,8 %); l'entreprise ne voulait pas investir plus de temps et d'argent dans l'incident (14,2 %); ou l'entreprise ne croyait pas que l'auteur serait puni adéquatement ou déclaré coupable (12,3 %) (voir le tableau 2A à l'annexe A).

Les grandes entreprises s'abstiennent de signaler les cyberincidents pour des raisons différentes de celles des petites et moyennes entreprises

Il y a quelques ressemblances et différences dans les raisons de ne pas signaler les cyberincidents à la police selon la taille de l'entreprise (voir le tableau 2A à l'annexe A). Par exemple, les grandes entreprises (70,3 %) étaient plus susceptibles d'indiquer avoir résolu les incidents à l'interne que les moyennes (55,3 %) ou petites entreprises (50,0 %). De même, les incidents étaient plus souvent résolus par l'intermédiaire d'un consultant en TI dans les petites (33,5 %) et moyennes entreprises (32,4 %) que dans les grandes entreprises (18,0 %). Ces dernières (42,2 %) étaient plus susceptibles d'indiquer que le cyberincident était trop mineur pour être signalé à la police que les petites (25,4 %) et moyennes entreprises (38,7 %). Un plus grande nombre de petites entreprises (24,6 %) ont indiqué qu'elles n'avaient pas pensé à appeler la police pour signaler l'incident comparativement aux moyennes (21,6 %) ou grandes entreprises (15,0 %). Enfin, près du quart des grandes entreprises (23,0 %) ne croyaient pas que la police considérerait l'incident comme important, comparativement à 20,8 % des moyennes entreprises et à 18,0 % des petites entreprises.

Prédire le signalement des incidents à la police

Les entreprises qui signalent les cyberincidents ont mis en place un plus grand nombre de mécanismes de protection

Les entreprises qui avaient signalé les cyberincidents à la police tendaient à avoir mis en place plus de protocoles de gestion des risques, de mécanismes de formation officielle et de mesures de cybersécurité, et à avoir communiqué des pratiques exemplaires aux employés et aux TI, comparativement aux entreprises qui n'avaient pas signalé de cyberincidents à la police (voir le tableau 3A à l'annexe A).

Les analyses de régression logistique ont confirmé l'importance des protocoles de gestion des risques, de la formation officielle, des mesures de cybersécurité, des pratiques exemplaires et de la taille de l'entreprise lorsqu'il s'agit de prédire la probabilité qu'une entreprise signale les cyberincidents à la police (voir le tableau 4A à l'annexe A).

La taille de l’entreprise influence quand et pourquoi les incidents sont signalés à la police

La taille d’une entreprise influençait elle aussi la probabilité de signaler un cybercrime à la police, les grandes et moyennes entreprises étant plus susceptibles d’effectuer un signalement que les petites entreprises (voir le tableau 4A à l’annexe A). Les grandes entreprises étaient plus susceptibles de signaler un cybercrime à la police lorsqu’elles mettaient en œuvre moins de mesures de sécurité, tandis que dans le cas des petites entreprises, les scores aux mesures de sécurité n’avaient rien à voir avec le signalement à la police. Les petites entreprises étaient moins susceptibles de signaler un cybercrime à la police lorsqu’elles mettaient en œuvre des pratiques exemplaires. Les grandes et petites entreprises étaient toutes deux plus susceptibles de signaler un cybercrime à la police lorsqu’elles mettaient en place un plus grand nombre de mesures de formation officielle. Enfin, toutes les entreprises (quelle que soit leur taille) étaient plus susceptibles de signaler un cybercrime à la police lorsqu’elles mettaient en œuvre un plus grand nombre de pratiques de gestion des risques.

Discussion

Étant donné la dépendance accrue à la technologie, les entreprises se préoccupent de plus en plus de la sécurité de leurs systèmes et de leur réseau (Kaplan et al., 2011; Kshetri, 2010). Or la recherche révèle que les cyberinfractions sont sous-signalées (Kethineni et Cao, 2019; Rantala, 2008; Statistique Canada, 2018a; Sukhai, 2004), bien qu’on ignore le niveau exact de cybercrime au Canada et qu’on ne connaisse pas bien les raisons pour lesquelles les incidents de cybersécurité ne sont pas signalés, surtout dans un contexte canadien. C’est pourquoi la présente étude avait pour but d’examiner le nombre d’entreprises qui signalent les cybercrimes aux autorités, les motifs de signalement et les caractéristiques des entreprises qui signalent les cybercrimes comparativement à celles qui ne le font pas, et ce à partir des données de l’Enquête canadienne sur la cybersécurité et le cybercrime de 2017, menée auprès d’entreprises canadiennes.

Sommaire des résultats

Dans l’ensemble, les résultats indiquent que tout juste plus de 20 % des entreprises sont victimes d’un cyberincident, les grandes entreprises étant victimes d’un plus grand nombre de cyberincidents que les petites entreprises; toutefois, très peu d’entreprises signalent ces incidents à la police, et ce pour les raisons suivantes : la majorité des incidents sont résolus à l’interne ou par l’intermédiaire de consultants en TI, l’incident est jugé trop mineur pour être signalé, ou les entreprises ne pensent pas à faire un signalement à la police (c.-à-d. qu’elles ne pensent pas à communiquer avec la police).

En général, la gestion des risques, la formation officielle et la communication des pratiques exemplaires sont associées au signalement des incidents à la police. Plus précisément, la probabilité de signaler les incidents à la police augmente avec le renforcement des protocoles de gestion des risques et mécanismes de formation officielle des entreprises. En revanche, il est intéressant de noter que plus les pratiques exemplaires sont communiquées, moins il est probable qu’un signalement soit fait à la police. Cette dernière constatation pourrait toutefois être due au

fait que la variable des pratiques exemplaires repose sur seulement deux questions, qui ne suffisent peut-être pas à bien mesurer la communication des pratiques exemplaires au sein des entreprises.

Répercussions stratégiques

Les taux élevés de cyberincidents dont sont victimes les entreprises canadiennes laissent entrevoir l'importance d'accroître la sensibilisation à la fréquence des cybercrimes et à la nécessité pour les entreprises d'améliorer leur cybersécurité. Si les petites entreprises ne disposent peut-être pas des ressources nécessaires pour offrir une formation officielle à leurs employés et au personnel des TI, il est néanmoins important d'accroître la sensibilisation aux options et aux programmes de formation officielle qui pourraient être généralement accessibles aux entreprises en matière de cybersécurité.

C'est notamment parce qu'elles ne croyaient pas que la police considérerait l'incident comme important que les entreprises n'avaient pas signalé les cybercrimes (quelque 20 % des entreprises ont donné cette raison pour ne pas avoir effectué de signalement à la police). Environ 20 % des entreprises ont aussi indiqué qu'elles n'avaient pas pensé à communiquer avec la police au sujet des cyberincidents. Comme de nombreuses entreprises n'avaient pas signalé les incidents à la police en raison du niveau de gravité (p. ex., incident mineur), on peut en conclure que ces entreprises ne comprennent peut-être pas toutes les répercussions criminelles que peuvent avoir les cyberincidents, ce qui indique qu'il faudrait en faire davantage pour accroître la sensibilisation. Ainsi, une plus grande sensibilisation du public est requise quant à l'importance d'effectuer des signalements à la police, même si l'incident est considéré comme mineur. Puisque les petites entreprises sont les moins susceptibles de signaler les cyberincidents, ce sont peut-être elles que les mesures de sensibilisation devraient cibler. De plus, les futurs programmes et politiques pourraient trouver un moyen d'inciter les entreprises à effectuer des signalements à la police.

Limites et orientations futures

Comme il s'agit de la première enquête nationale menée par Statistique Canada sur le cybercrime et la cybersécurité, il convient de mentionner certaines limites. Par exemple, il n'a pas été possible de subdiviser les résultats par type d'industrie en raison du petit échantillon d'entreprises qui avaient signalé des incidents à la police. Ainsi, de plus amples recherches sont requises pour examiner les différences entre les types d'industrie sur le plan de la fréquence des signalements à la police, des motifs de signalement à la police et des variables qui pourraient influencer la décision des entreprises de signaler les incidents à la police (p. ex., plus de formation officielle). De futures versions de l'ECCSCC sont également nécessaires pour examiner comment le signalement à la police pourrait changer au fil du temps et selon la taille et le type d'entreprise, ce qui permettrait de cerner les lacunes dans les services offerts et les politiques adoptées, surtout compte tenu de l'évolution constante du monde cybernétique. Il faudrait en outre mener de plus amples recherches sur les entreprises qui signalent les incidents à des tiers comparativement aux entreprises qui signalent les incidents à la police, afin de se faire une meilleure idée de la réaction des entreprises aux cyberincidents. Enfin, il serait pertinent de distinguer les cybercrimes selon qu'ils sont d'origine interne ou externe.

Conclusion

La présente étude aide à comprendre pourquoi certaines entreprises sont plus susceptibles d'effectuer des signalements à la police et quels types d'incidents sont signalés. Fait important, le dixième seulement de toutes les entreprises qui ont été victimes d'un incident l'ont signalé à la police. En comprenant non seulement les raisons pourquoi les entreprises ne signalent pas les incidents, mais aussi les facteurs qui pourraient accroître la probabilité que des signalements soient faits à la police, on peut se faire une meilleure idée des entreprises qui courent un plus grand risque d'être victimes d'un cyberincident, et cibler les entreprises appropriées lorsqu'il s'agit des efforts de prévention, de la prestation des services et des campagnes de sensibilisation. L'ECCSCC est la première enquête en son genre et présente des renseignements utiles aux entreprises, aux gouvernements et à la population générale du Canada. L'examen des données provenant de ses futures versions aidera à déchiffrer les tendances, en plus d'orienter les efforts en matière de recherche et de politiques.

Références

AON. (2019, février). *2019 Cyber Security Risk Report: What's Now and What's Next*. Repéré à https://www.aon.com/mwginternal/de5fs23hu73ds/progress?id=tHMHtR8 q0_OmcVHKqQhUwNWef9bxKiiL99rvl3blz4,&dl

Department for Digital, Culture, Media and Sport. (2018). *Cyber Security Breaches Survey 2018: Statistical Release*. Department for Digital, Culture, Media and Sport. Royaume-Uni.

Kaplan, J., Sharma, S. et Weinberg, A. (2011, juin). *Meeting the Cybersecurity Challenge.* Repéré à https://www.mckinsey.com/business-functions/digitalmckinsey/our-insights/meeting-the-cybersecurity-challenge

Keizer, G. (2006, janvier). *Cybercrime feared 3 times more than physical crime*. Semaine de l'information.

Kethineni, S. et Cao, Y. (2019). The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review* (Prépublication en ligne), 1-20. doi: 10.1177/1057567719827051

Khalid, A. (2004, mars). Cyber crime: Business and the law on different pages. *The Star*. Repéré à http://www.niser.org.my/news/2004_03_05_01.html

Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. New York, NY : Springer. doi: 10.1007/978-3-642-11522-6

McAfee. (2018, février). *The Economic Impact of Cybercrime—No Slowing Down.* Santa Clara, CA. Repéré à https://www.mcafee.com/enterprise/eus/assets/executive-summaries/es-economic-impact-cybercrime.pdf

Norton. (2018). *2017 Norton Cyber Security Insights Report: United States Results.* Symantec, CA : États-Unis. Repéré à https://www.symantec.com/content/dam/symantec/docs/about/ 2017-ncsir-united-states-results-en.pdf

Rantala, R. R. (2008, septembre). *Cybercrime Against Businesses, 2005.* Washington, D.C. : États-Unis. Department of Justice; Bureau of Justice Statistics. Repéré à http://www.justiceacademy.org/iShare/Library-BJS/CyberCrimes.pdf

Soloman, H. (2016, juin). *Firms too scared to report cyber crime, says police investigator.* IT World Canada : Toronto, Ontario. Repéré à https://www.itworldcanada.com/article/firms-too-scared-to-report-cyber-crime-says-police-investigator/383747

Soloman, H. (2018, février). *Cyber crime costs the world almost US$600 billion a year: Report.* IT World Canada : Toronto, Ontario. Repéré à https://www.itworldcanada.com/article/cyber-crime-costs-the-world-almost-us600-billion-a-year-report/402038

Statistique Canada. (2018a, octobre). *Le Quotidien : L'incidence du cybercrime sur les entreprises canadiennes, 2017.* Ottawa, Ontario. Repéré à https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-fra.htm

Statistique Canada. (2018b). *Enquête canadienne sur la cybersécurité et le cybercrime*. Ottawa, Ontario. Repéré à http://www23.statcan.gc.ca/imdb/p3Instr_f.pl?Function=assembleInstr&Item_Id=418254

Sukhai, N. B. (2004, octobre). Hacking and Cybercrime. Dans *Proceedings from the 1st Annual Conference on Information Security Curriculum Development* à Kennesaw, GA. doi: 10.1145/1059524.1059553

Annexe A – Tableaux sommaires

Tableau 1A

Fréquence des cyberincidents et de leur signalement à la police selon la taille de l'entreprise

Fréquence	Total %	Taille de l'entreprise		
		Petite %	Moyenne %	Grande %
A été victime d'un cyberincident	20,8	18,8	28,0	41,0
A signalé un cyberincident à la police	9,6	8,4	12,5	15,0
A signalé tous les cyberincidents dont elle a été victime à la police	6,3	6,3	6,2	7,6

Nota. Les entreprises étaient considérées comme petites si elles comptaient de 10 à 49 employés, moyennes si elles comptaient de 50 à 249 employés, et grandes si elles comptaient 250 employés ou plus.

Tableau 2A

Comparer les raisons pourquoi les entreprises n'ont pas signalé les cyberincidents à la police pour les petites, moyennes et grandes entreprises

Motif de non-signalement à la police	Total	Taille de l'entreprise			
		Petite	Moyenne	Grande	
	%	%	%	%	*F*
Incident résolu à l'interne	52,1	50,0	55,3	70,3	221,38**
Incident résolu par l'intermédiaire d'un consultant en TI	32,5	33,5	32,4	18,0	113,64**
Incident trop mineur	29,1	25,4	38,7	42,2	196,78**
N'a pas pensé à communiquer avec la police	23,5	24,6	21,6	15,0	143,73**
Ne croyait pas que la police considérerait l'incident comme important	18,8	18,0	20,8	23,0	170,02**
Ne voulait pas investir plus de temps ou d'argent dans la question	14,2	15,2	11,4	12,2	155,72**
Ne croyait pas que l'auteur serait puni adéquatement	12,3	13,2	9,9	8,5	158,09**
Manque de données probantes	9,3	8,2	12,8	10,0	173,34**
Processus de signalement trop compliqué	3,8	3,8	3,7	4,4	174,00**
Réponse de la police insatisfaisante par le passé	2,5	2,3	2,9	3,8	176,33**

Nota. Les motifs de non-signalement ne sont pas mutuellement exclusifs; les entreprises pourraient indiquer plusieurs raisons de ne pas avoir signalé les incidents à la police. Par conséquent, la somme des pourcentages ne correspond pas à 100 %. Les entreprises étaient considérées comme petites si elles comptaient de 10 à 49 employés, moyennes si elles comptaient de 50 à 249 employés, et grandes si elles comptaient 250 employés ou plus. $^{**}p < 0{,}001$.

Tableau 3A

Comparer les scores à divers mécanismes de protection cybernétique entre les entreprises qui ont signalé un incident et celles qui n'ont pas signalé d'incident

Mécanismes de protection	**Ont signalé un incident**		**N'ont pas signalé d'incident**		***t***
	M	***SD***	***M***	***SD***	
Protocoles de gestion des risques (Fourchette : 0-7)	3,02	1,89	2,30	1,43	-28,41**
Formation officielle (Fourchette : 0-3)	1,04	1,01	0,50	0,83	-37,04**
Mesures de cybersécurité (Fourchette : 0-11)	7,03	2,90	6,29	2,98	-14,60**
Communication des pratiques exemplaires (Fourchette : 0-2)	1,29	0,91	1,18	0,87	-7,11**

Nota. M = moyenne. *SD* = écart-type. *t* = résultats aux tests t. Le tableau porte sur les incidents signalés à la police, et non sur les incidents signalés à des tiers. ***p* < 0,001.

Tableau 4A

Résultats des analyses de régression logistique prédisant la probabilité que les entreprises signalent les cyberincidents à la police

Prédicteurs	***b* (*SE*)**	**χ^2**	**RC**	**IC à 95 %**
Protocoles de gestion des risques	0,20 (0,02)	121,64***	1,22	[1,18; 1,26]
Formation officielle offerte	0,60 (0,03)	482,86***	1,83	[1,73; 1,93]
Mesures de cybersécurité	-0,01 (0,01)	0,35	1,00	[1,00; 1,01]
Communication des pratiques exemplaires	-0,44 (0,03)	203,74***	1,55	[1,46; 1,64]
Taille de l'entreprise	0,30 (0,05)	38,28***	1,34	[1,22; 1,48]
Interactions				
Gestion des risques x taille de l'entreprise	-0,02 (0,03)	0,59	1,02	[0,97; 1,08]
Formation officielle x taille de l'entreprise	-0,11 (0,05)	6,14*	1,12	[1,02; 1,22]
Mesures de sécurité x taille de l'entreprise	-0,08 (0,02)	20,87***	1,08	[1,05; 1,12]
Pratiques exemplaires x taille de l'entreprise	0,55 (0,07)	73,10***	1,74	[1,53; 1,97]

Nota. b = coefficient de régression. *SE* = erreur-type. χ^2 = chi carré de Wald. RC = rapport des cotes. IC = intervalle de confiance. *$p < 0,05$. ***$p < 0,001$.