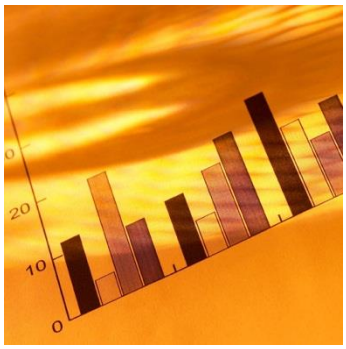
SOMMAIRE DE RECHERCHE

Profil des entreprises canadiennes qui signalent les cybercrimes à la police



2019–S006

www.securitepublique.gc.ca

BUILDING A SAFE AND RESILIENT CANADA

Tout juste plus de 20 % des entreprises ont été victimes de cyberincidents, mais seulement 10 % les ont signalés à la police. Les incidents étaient souvent résolus à l'interne ou par l'intermédiaire d'un consultant en TI, ou jugés trop mineurs pour être signalés.

Contexte

Le cybercrime (piratage informatique, propagation de virus et crime organisé commis au moyen d'un ordinateur) préoccupe de plus en plus les gouvernements, organisations, individus et entreprises partout dans le monde. Or on ignore le niveau exact de cybercrime au Canada; jusqu'à présent, la plupart des recherches examinant l'impact du cybercrime a été effectuée aux États-Unis.

Si la recherche montre que les cyberinfractions sont sous-signalées, ce phénomène peut s'expliquer par plusieurs raisons. 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.

Cette étude prend appui sur les données de l'Enquête canadienne sur la cybersécurité et le cybercrime de 2017 (ECCSCC). Cette dernière a été réalisée auprès d'entreprises canadiennes en 2018 dans le but de cerner le nombre 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 que ne le font pas.

Méthode

L'ECCSCC a été conçue par Statistique Canada en consultation avec divers organismes gouvernementaux (dont Sécurité publique Canada) ainsi que des services de police, des experts en la matière, des universitaires, des entreprises privées et des associations de gens d'affaires. Ce processus a permis de peaufiner le questionnaire jusqu'à obtenir les 35 questions utilisées pour l'étude, qui portait sur les incidents de sécurité survenus de janvier à décembre 2017.

Les données ont été collectées auprès d'entreprises canadiennes qui comptaient au moins dix employés, dans tous les secteurs sauf la fonction et l'administration publiques. 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 de 10 à 49 employés, 35,5 % des moyennes entreprises de 50 à 249 employés, et 19,6 % des grandes entreprises de 250 employés ou plus.

Diverses questions de l'Enquête portant sur le signalement des incidents à la police ont permis d'examiner la fréquence et d'effectuer des analyses de la variance pour les diverses tailles d'entreprise (et en général). 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. Enfin, des analyses de régression logistique ont permis de déterminer si les entreprises qui signalent les incidents de cybersécurité à la police présentent des caractéristiques distinctes.

Constatations

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. Toutefois, seulement 9,6 % des entreprises avaient signalé les incidents à la police (8,4 % des petites entreprises, 12,5 % des moyennes entreprises et 15,0 % des grandes entreprises).

Les incidents avaient souvent été résolus à l'interne (52,1 %), résolus par l'intermédiaire d'un consultant en TI (32,5 %) ou jugés trop mineurs pour être signalés à la police (29,1 %), ou encore les entreprises n'avaient pas pensé à communiquer avec la police (23,5 %).

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.

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, un moins grand nombre de mesures de sécurité n'avait 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.

Répercussions

Les constatations laissent entrevoir la nécessité pour les entreprises d'améliorer leurs mesures de cybersécurité, de même que l'importance d'accroître la sensibilisation à la fréquence des cybercrimes, puisqu'une entreprise canadienne sur cinq en a été victime. Il faudrait en outre sensibiliser davantage le public à l'importance d'effectuer des signalements à la police, et ce même si l'incident peut sembler mineur.

Comme les petites entreprises sont les moins susceptibles de signaler les cyberincidents à la police, ce sont peut-être elles que les mesures de sensibilisation devraient cibler. De plus, les futurs programmes et politiques pourraient trouver des moyens d'inciter les entreprises à effectuer des signalements à la police.

Enfin, il faudrait mener de plus amples recherches en vue de comparer les entreprises qui signalent les incidents à des tiers avec les entreprises qui signalent les incidents à la police, afin de se faire une meilleure idée de la réaction des entreprises aux cyberincidents.

Source

Wanamaker, K. A. (2019). *Profil des entreprises canadiennes qui signalent les cybercrimes à la police : L'Enquête canadienne sur la cybersécurité et le cybercrime de 2017*. Ottawa, Ontario : Sécurité publique Canada.

Sources additionnelles

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

Pour obtenir davantage de renseignements sur la recherche effectuée au Secteur de la sécurité communautaire et de la réduction du crime de Sécurité publique Canada, pour obtenir une copie du rapport de recherche complet ou pour être inscrit à notre liste de distribution, veuillez communiquer avec :

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

2019–S006

ISSN : 1916-4009

Les sommaires de recherche sont produits pour le Secteur de la sécurité communautaire et de la réduction du crime, Sécurité publique Canada. Les opinions exprimées dans le présent sommaire sont celles des auteurs et ne reflètent pas nécessairement celles de Sécurité publique Canada.

2019–S006

ISSN : 1916-4009