Nº 22200001 au catalogue
ISBN 978-0-660-48649-9

Aperçus numériques

Le paysage changeant de la cybersécurité à la suite de la pandémie de COVID-19

par Gabrielle Asselin et Howard Bilodeau

Date de diffusion : le 11 juillet 2023

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 infostats@statcan.gc.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

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.

Le paysage changeant de la cybersécurité à la suite de la pandémie de COVID-19

par **Gabrielle Asselin** et **Howard Bilodeau**

Les changements sociaux accélérés par la pandémie de COVID-19 ont eu des répercussions sans précédent sur les activités des entreprises au Canada; de nombreuses entreprises ont modifié leurs modèles d'affaires et ont commencé à utiliser Internet et d'autres technologies d'une nouvelle manière. Selon l'Enquête sur la technologie numérique et l'utilisation d'Internet, le tiers (33 %) des entreprises canadiennes ont reçu des commandes ou vendu des produits ou des services au moyen d'Internet en 2021, en hausse de 25 % par rapport à 2019, avant la pandémie. Davantage d'entreprises ont également déclaré offrir à leurs employés l'option de faire du télétravail en 2021 par rapport à 2019 (+14 points de pourcentage)[1].

Bien qu'une présence croissante en ligne ait créé de nouvelles occasions pour de nombreuses entreprises, elle les a également exposées à de nouveaux risques en matière de protection de la vie privée, de protection des données et de cybersécurité. De nombreux types de crimes qui ont fait la une des journaux en 2021, y compris le cybercrime, la fraude et la contrefaçon, ne sont pas nouveaux; ce sont plutôt des types de crimes existants et les gens qui les ont commis ont su tirer profit des avancées technologiques pour peaufiner leurs techniques[2]. Le présent article porte sur les façons dont les entreprises canadiennes s'adaptent aux menaces à la cybersécurité dans la foulée de la pandémie au moyen des données de l'Enquête canadienne sur la cybersécurité et le cybercrime (ECCC)[3].

Les entreprises canadiennes prennent davantage de cyberprécautions

En 2021, 26 % des entreprises canadiennes avaient des politiques écrites en lien avec la cybersécurité, une augmentation d'au moins 4 points de pourcentage par rapport à 2019[4]. Cela indique que les entreprises prennent de plus en plus conscience des menaces posées par les incidents en cybersécurité.

Les entreprises ont également fait preuve d'une sensibilisation croissante en matière de cybersécurité par d'autres moyens; par exemple, la proportion d'entreprises menant des activités visant à identifier les risques de cybersécurité de manière régulière a augmenté de cinq points de pourcentage pour atteindre 39 % en 2021. Selon les données du deuxième trimestre de 2022 de l'Enquête canadienne sur la situation des entreprises, le cinquième (21 %) des établissements canadiens projettent de mettre en œuvre des mesures de cybersécurité nouvelles ou supplémentaires au cours des 12 prochains mois[5].

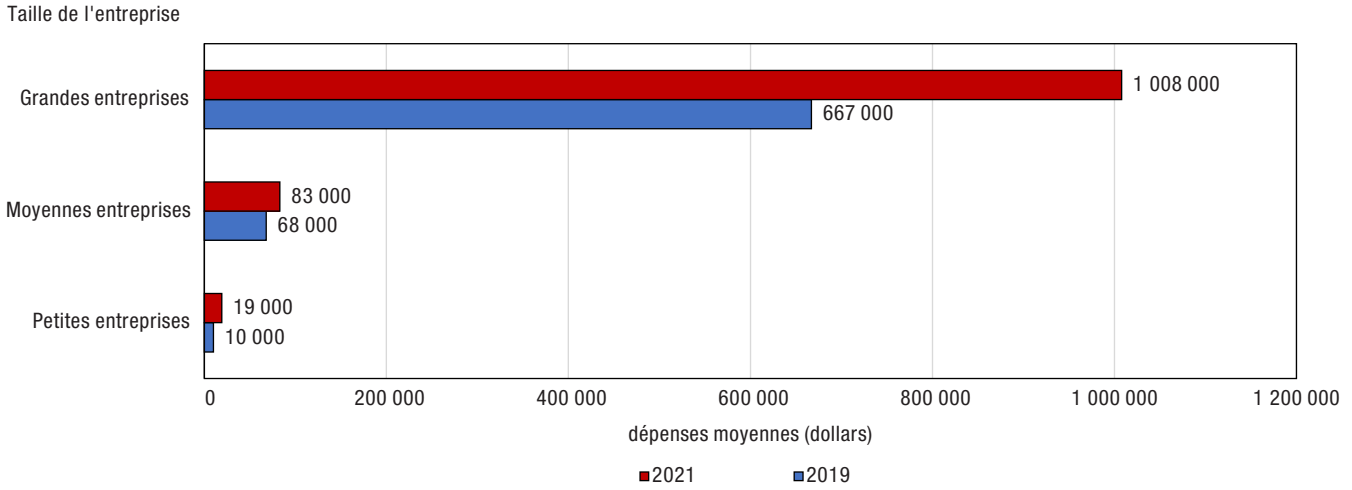
Les entreprises canadiennes dépensent davantage en prévention et en détection des incidents de cybersécurité

L'augmentation apparente de la sensibilisation des entreprises canadiennes à la cybersécurité s'est également reflétée dans les dépenses en cybersécurité. En 2021, les dépenses moyennes en prévention et en détection des incidents de cybersécurité se sont chiffrées à 52 000 $; il s'agit d'une hausse considérable de 46 % par rapport à 2019, qui a largement dépassé le taux d'inflation observé au cours de la même période (+4 %)[6]. En 2021, les grandes entreprises ont dépensé environ 340 000 $ de plus en prévention et en détection des incidents de cybersécurité qu'elles ne l'ont fait en 2019, tandis que les petites entreprises ont déboursé environ 9 000 $ de

1. Un article dans lequel les résultats de 2021 de l'Enquête sur la technologie numérique et l'utilisation d'Internet sont mis en évidence a été diffusé dans *Le Quotidien* le 13 septembre 2022. Un article connexe fondé sur les données de la même enquête, intitulé « Changements apportés aux stratégies de commerce électronique des entreprises canadiennes pendant la pandémie de COVID-19 » a été diffusé le 29 novembre 2022.
2. Données de la Commission européenne (en anglais seulement) : Guide to statistics in European Commission development cooperation—2021 edition—Volume 2: Population and social statistics.
3. Les résultats de l'Enquête canadienne sur la cybersécurité et le cybercrime de 2021 ont été diffusés dans *Le Quotidien* le 18 octobre 2022. Le présent article précise les tendances présentées dans l'article publié dans *Le Quotidien*.
4. Les statistiques relatives aux politiques écrites liées à la cybersécurité sont dérivées de la question 12 des versions 2019 et 2021 de l'ECCC. Certaines catégories de réponses à cette question ont été reformulées ou divisées en 2021, et une nouvelle catégorie "autre type de politique écrite liée à la cybersécurité" a été ajoutée. Si l'on exclut la nouvelle catégorie "autre", l'augmentation de l'adoption de politiques écrites entre 2019 et 2021 est de quatre points de pourcentage.
5. Données de l'Enquête canadienne sur la situation des entreprises : Plans de l'entreprise ou de l'organisme quant à la mise en œuvre de nouvelles mesures ou de mesures supplémentaires de cybersécurité au cours des 12 prochains mois, deuxième trimestre de 2022. L'Enquête canadienne sur la situation des entreprises vise les établissements, tandis que l'ECCC vise les entreprises. Une entreprise peut avoir plusieurs établissements, alors il faut faire preuve de prudence lorsque l'on compare les deux sources de données.
6. Données de l'Indice moyen annuel des prix à la consommation.

plus. Cependant, l'augmentation de la sensibilisation à la cybersécurité pourrait ne pas se manifester de manière uniforme à l'échelle de l'économie; 4 entreprises sur 10 n'ont toujours pas déclaré de dépenses directes en cybersécurité en 2021. Ce chiffre n'a pas changé depuis 2019.

Graphique 1
Montant moyen dépensé en prévention et en détection des incidents de cybersécurité, selon la taille de l'entreprise, 2019 et 2021



Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime, 2019 et 2021.

Une partie de la motivation de certaines entreprises à investir davantage en cyberdéfense et en politiques pourrait être la sensibilisation parallèle des consommateurs à l'égard des risques de communiquer leurs renseignements personnels lorsqu'ils font des achats en ligne. Selon l'Enquête canadienne sur l'utilisation d'Internet de 2020, le quart (25 %) des personnes canadiennes étaient très ou extrêmement préoccupées par la cybersécurité ou les menaces à la vie privée pendant l'utilisation de sites ou d'applications d'achats en ligne[7]. De même, selon l'ECCC de 2021, la protection des renseignements personnels a été la raison la plus fréquemment invoquée par les entreprises pour dépenser de l'argent ou passer du temps sur la cybersécurité. Les deux tiers (66 %) de celles-ci ont choisi cette réponse.

Bien que les entreprises fassent preuve d'une sensibilisation croissante à la cybersécurité dans certains domaines de leurs activités, la tendance n'est pas universelle ; la proportion d'entreprises disposant d'employés dédiés à la cybersécurité est restée largement inchangée entre 2019 (60 %) et 2021 (61 %), et seulement un peu plus d'entreprises ont fourni une formation formelle pour développer ou mettre à niveau les compétences en cybersécurité de leurs employés ne travaillant pas dans le domaine des technologies de l'information en 2021 (+3 points de pourcentage). Depuis longtemps, l'erreur humaine est reconnue comme étant une source majeure d'incidents en cybersécurité; le perfectionnement des connaissances en cybersécurité de l'ensemble des employés peut donc jouer un rôle majeur dans l'amélioration de la cyberrésilience opérationnelle[8].

Un moins grand nombre d'entreprises canadiennes ont été touchées par des incidents de cybersécurité en 2021, mais les coûts déclarés des incidents ont augmenté

Un nombre légèrement inférieur d'entreprises canadiennes (18 %) ont déclaré avoir été touchées par un incident de cybersécurité en 2021 par rapport à 2019 (21 %). Cette tendance diffère de celle observée pour les personnes canadiennes dans l'Enquête canadienne sur l'utilisation d'Internet de 2020, dans laquelle le pourcentage de personnes touchées par des incidents de cybersécurité a progressé de 6 points de pourcentage de 2018 à

7. Données de l'Enquête canadienne sur l'utilisation d'Internet : Niveau de préoccupation concernant les menaces pour la sécurité et la vie privée lors de l'utilisation d'applications ou de technologies numériques.
8. Résultats du rapport sur les risques mondiaux de 2022 (en anglais seulement) du Forum économique mondial.

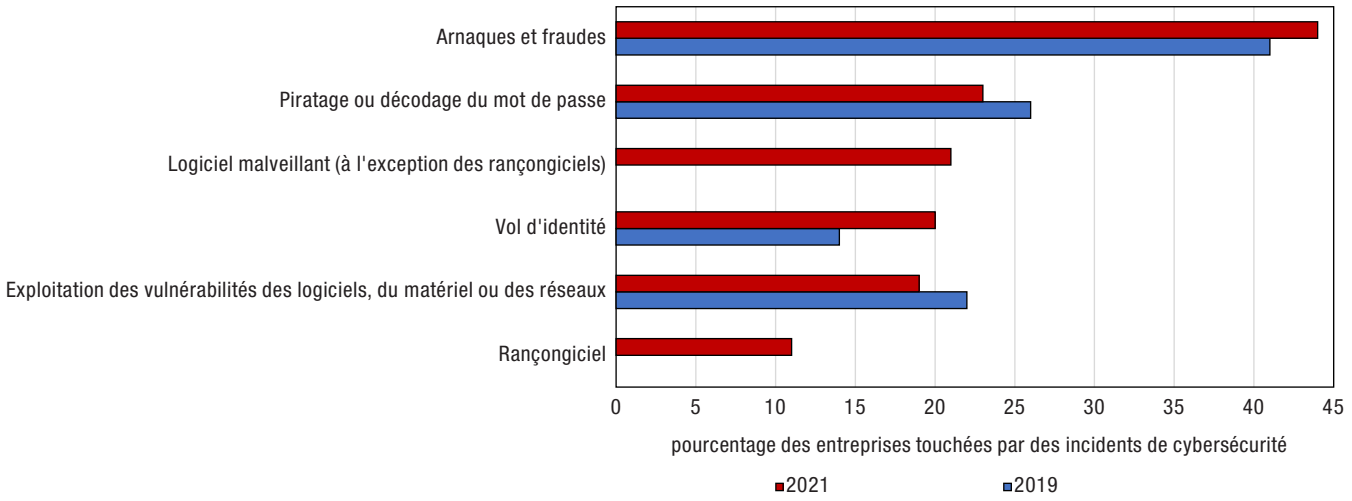
2020 pour atteindre 58 %[9]. Ces tendances pourraient rendre compte d'une modification des stratégies des cybercriminels, mais elles pourraient également découler du fait que les entreprises ont accès à plus d'outils que les personnes pour identifier et intercepter les cyberactivités malveillantes.

Bien que des preuves indiquant que les entreprises sont de plus en plus sensibilisées à la cybersécurité aient été présentées dans les parties précédentes, celles qui ont été touchées par des incidents de cybersécurité en 2021 ont subi des conséquences financières plus importantes par rapport à 2019. En moyenne, en 2021, les entreprises ont déboursé 19 000 $ pour rétablir leurs des activités à la suite d'incidents de cybersécurité. Il s'agit de 8 000 $ de plus qu'en 2019 (11 000 $). Cette augmentation est en grande partie due à une hausse substantielle des coûts supportés par les grandes entreprises entre 2019 (73 000 $) et 2021 (172 000 $).

Les entreprises qui avaient des politiques écrites en matière de cybersécurité sont également plus susceptibles d'être touchées par des incidents de cybersécurité (25 %) que celles qui n'ont pas de politiques (16 %) en 2021. Cette constatation pourrait s'expliquer par le fait que les entreprises sensibilisées à la cybersécurité sont mieux placées pour remarquer les incidents de cybersécurité que celles qui n'ont pas mis en place de procédures de surveillance. Les entreprises qui sont plus souvent la cible d'incidents de cybersécurité peuvent également être plus susceptibles d'adopter des politiques écrites en matière de cybersécurité. En outre, bien que les entreprises disposant de politiques écrites aient été touchées par des incidents de cybersécurité à un taux plus élevé que celles qui n'en disposent pas, il y avait encore plus d'entreprises sans politique écrite touchées par des incidents (22 000) que d'entreprises disposant de politiques écrites (12 000) en 2021. Cela s'explique en partie par le fait que 74 % des entreprises n'ont pas de politique écrite en place.

Parmi les entreprises touchées par des incidents de cybersécurité, le vol d'identité a connu la plus forte hausse en 2021 par rapport à 2019 (en hausse de 6 points de pourcentage pour se chiffrer à 20 %). À l'inverse, les proportions des entreprises qui ont déclaré avoir été touchées par le piratage ou le décodage d'un mot de passe (-3 points de pourcentage) et par l'exploitation des vulnérabilités des logiciels, du matériel ou des réseaux (-3 points de pourcentage) ont reculé en 2021. Mesuré pour la première fois en 2021 comme une catégorie à part entière, 11 % des entreprises canadiennes qui ont été touchées par un incident de cybersécurité ont déclaré avoir été touchées par un rançongiciel[10].

Graphique 2
Méthodes utilisées pour les incidents de cybersécurité, entreprises touchées par des incidents de cybersécurité, 2019 et 2021



Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime, 2019 et 2021.

9. Données de l'Enquête canadienne sur l'utilisation d'Internet : Enquête canadienne sur l'utilisation d'Internet, 2020.
10. Avant le cycle de 2021 de l'Enquête canadienne sur la cybersécurité et le cybercrime, les rançongiciels étaient compris dans la catégorie des logiciels malveillants.

Portail de statistiques sur l'économie et la société numériques

Visitez le portail Statistiques sur l'économie et la société numériques pour accéder, en un seul endroit pratique, aux données, aux publications et aux outils interactifs liés à l'économie et à la société numériques.

Méthodologie

Les données utilisées dans le présent article proviennent de l'Enquête canadienne sur la cybersécurité et le cybercrime (ECCC), sauf indication contraire.

Les données du cycle de 2021 de l'ECCC ont été recueillies de janvier à mars 2022. La population cible de l'enquête a été sélectionnée à partir du Registre des entreprises (RE) de Statistique Canada. Le RE est une base de données sur la population des entreprises canadiennes et il sert de base de sondage à toutes les enquêtes-entreprises de Statistique Canada. Il s'agit d'une liste structurée d'entreprises productrices de biens et de services au Canada. Cette enquête vise les entreprises exerçant des activités au Canada dans presque tous les secteurs industriels. Les entreprises comptant moins de 10 employés ont été exclues de l'échantillon. L'échantillon final comprenait 12 158 entreprises et le taux de réponse était de 65 %.

Afin de créer l'échantillon pour l'enquête, les entreprises ont été stratifiées par industrie et par catégorie de taille. La catégorie de taille est fondée sur le nombre d'employés de l'entreprise. Trois catégories de taille ont été créées : petite (de 10 à 49 employés), moyenne (de 50 à 249 employés) et grande (250 employés ou plus).

Les pourcentages publiés dans le présent article représentent un pourcentage des entreprises, sauf indication contraire. Des poids de sondage ont été utilisés dans tous les calculs pour garantir que les résultats rendent fidèlement compte de la population cible. Les changements de points de pourcentage par rapport à l'ECCC ne sont donnés que pour les proportions avec une qualité "A" (erreur standard jusqu'à 2,5 %).

Remerciements

L'ECCC est menée pour le compte de Sécurité publique Canada. Les auteurs tiennent à remercier les collègues de Sécurité publique Canada pour leurs conseils et leurs commentaires sur une version antérieure de cet article.

Références externes

Commission européenne (2021). Guide to statistics in European Commission development cooperation, Volume 2: Social statistics (en anglais seulement). Site consulté le 16 mars 2023.

Forum économique mondial (2022). The Global Risks Report 2022, 17th Edition, Insight Report (en anglais seulement). Site consulté le 16 mars 2023.