

Environ un cinquième des entreprises canadiennes ont été touchées par des incidents de cybersécurité en 2019

Diffusé à 8 h 30, heure de l'Est dans Le Quotidien, le mardi 20 octobre 2020

Cette diffusion coïncide avec le Mois de la sensibilisation à la cybersécurité, qui est une campagne internationale qui se déroule chaque année en octobre en vue d'informer le public de l'importance de la cybersécurité.

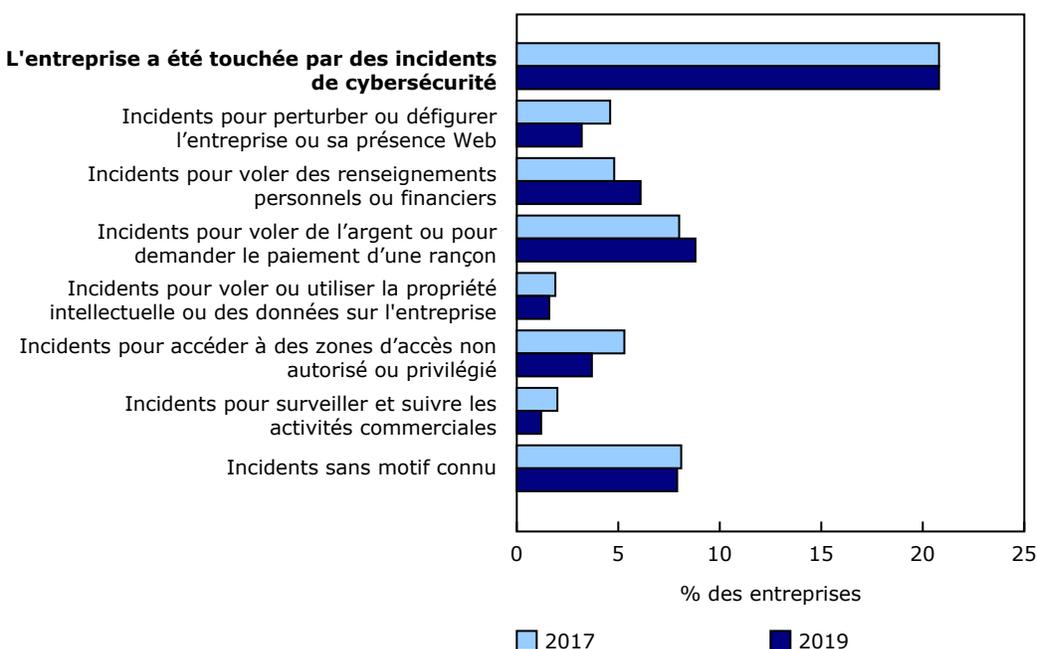
Bien que plusieurs incidents de cybersécurité importants aient été dévoilés publiquement par des entreprises canadiennes en 2019, environ un cinquième (21 %) de l'ensemble des entreprises canadiennes a déclaré avoir été touché par des incidents de cybersécurité, soit la même proportion qu'en 2017. Plus des deux cinquièmes (43 %) des grandes entreprises (250 employés ou plus) ont été touchées par des incidents de cybersécurité en 2019, comparativement à 29 % des moyennes entreprises (de 50 à 249 employés) et à 18 % des petites entreprises (de 10 à 49 employés).

Les secteurs industriels qui ont le plus souvent déclaré avoir été touchés par des incidents de cybersécurité en 2019 étaient le secteur de l'industrie de l'information et de l'industrie culturelle (37 % en 2019 par rapport à 30 % en 2017), celui du commerce de gros (34 % en 2019 par rapport à 27 % en 2017) et celui des services professionnels, scientifiques et techniques (32 % en 2019 par rapport à 27 % en 2017).

Les deux motifs d'incident le plus souvent mentionnés par les entreprises touchées par des incidents de cybersécurité en 2019 étaient les mêmes qu'en 2017. En 2019, 9 % des entreprises ont indiqué avoir été touchées par une tentative de vol d'argent ou une demande de paiement de rançon, et 8 % ont déclaré avoir été touchées par un incident sans motif connu. Le motif d'incident qui arrivait en troisième position en 2019 était la tentative de vol de renseignements personnels ou financiers (6 %).



Graphique 1 Types d'incidents de cybersécurité qui ont touché les entreprises, Canada



Source(s) : Enquête canadienne sur la cybersécurité et le cybercrime (5244).

Même si les motifs liés au vol d'argent ou de renseignements financiers étaient courants en 2019, un total de 12 % des entreprises touchées par des incidents de cybersécurité ont déclaré avoir perdu des revenus et 3 % ont indiqué avoir payé une rançon.

La plupart des entreprises canadiennes continuent de ne pas signaler les incidents de cybersécurité aux services de police

Alors qu'un pourcentage un peu plus élevé d'entreprises canadiennes touchées par des incidents de cybersécurité ont signalé ces incidents aux services de police en 2019 (12 %) comparativement à 2017 (10 %), la plupart des entreprises continuent de ne pas signaler ces incidents aux services de police. Une plus grande proportion d'entreprises ayant signalé des incidents aux services de police ont indiqué qu'elles avaient des polices d'assurance (34 %) par rapport à la moyenne globale (17 %). Les entreprises ayant signalé des incidents de cybersécurité aux services de police ont aussi déclaré un coût moyen de 27 000 \$ pour se remettre de tels incidents, comparativement au coût moyen global de 11 000 \$.

Les raisons le plus souvent invoquées par les entreprises pour ne pas signaler des incidents aux services de police en 2019 ont été que les incidents ont été réglés à l'interne (49 %), les incidents étaient trop mineurs pour être signalés (31 %) ou les incidents ont été réglés par l'intermédiaire d'un expert-conseil ou d'un entrepreneur de la technologie de l'information (TI) (29 %).

Les entreprises canadiennes déclarent avoir dépensé un total de 7 milliards de dollars directement pour la cybersécurité en 2019

Les entreprises canadiennes ont déclaré avoir dépensé un total de 7 milliards de dollars en 2019 directement pour des mesures visant à prévenir et à détecter les incidents de cybersécurité, et à s'en remettre, ce qui représente moins de 1 % de leurs revenus totaux. Environ 2 milliards de dollars ont été consacrés à la portion des salaires des

employés liée à la cybersécurité, 2 milliards de dollars ont été investis dans des logiciels de cybersécurité et 1 milliard de dollars ont été dépensés pour payer des experts-conseils et des entrepreneurs en TI embauchés pour des raisons de cybersécurité. Les dépenses pour diverses autres mesures de prévention, de détection et de rétablissement ont représenté les 2 milliards de dollars restants du total des dépenses en cybersécurité.

Les dépenses directes annuelles moyennes en cybersécurité variaient grandement selon la taille de l'entreprise en 2019. En moyenne, les grandes entreprises ont dépensé 699 000 \$, les moyennes entreprises ont dépensé 74 000 \$ et les petites entreprises ont dépensé 11 000 \$. Près du tiers des petites entreprises (32 %) n'ont déclaré aucune dépense directe en cybersécurité, comparativement à 21 % des moyennes entreprises et à 19 % des grandes entreprises.

Un plus grand nombre d'entreprises canadiennes mettent en œuvre des politiques officielles en matière de cybersécurité

En 2019, 18 % des entreprises canadiennes avaient des politiques écrites en place pour gérer les risques en matière de cybersécurité ou pour signaler les incidents de cybersécurité. Il s'agit d'une augmentation par rapport aux 13 % des entreprises qui ont déclaré avoir de telles politiques en 2017. Des hausses d'utilisation de politiques écrites ont été affichées par les petites entreprises (14 % en 2019 par rapport à 10 % en 2017), les moyennes entreprises (29 % en 2019 par rapport à 23 % en 2017) et les grandes entreprises (58 % en 2019 par rapport à 51 % en 2017). Les augmentations observées dans le secteur de la finance et des assurances (57 % en 2019 par rapport à 48 % en 2017) et celui des services publics (47 % en 2019 par rapport à 36 % en 2017) ont aussi contribué à la hausse globale d'utilisation de politiques écrites.

Les entreprises étaient également plus nombreuses à avoir des polices d'assurance pour les protéger contre les risques et les menaces en matière de cybersécurité en 2019 (17 %) qu'en 2017 (9 %). La variation du pourcentage des grandes entreprises ayant une police d'assurance pour la cybersécurité était encore plus prononcée, passant de 24 % en 2017 à 38 % en 2019. La variation était également plus prononcée en ce qui concerne les entreprises du secteur de la finance et des assurances (55 % en 2019 par rapport à 41 % en 2017).

Les entreprises canadiennes continuent d'utiliser bon nombre des mêmes techniques de cybersécurité

La plupart des entreprises canadiennes continuent d'utiliser des logiciels contre les programmes malveillants (76 % en 2019 et en 2017), la sécurité des courriels (73 % en 2019 par rapport à 74 % en 2017) et la sécurité des réseaux (69 % en 2019 par rapport à 68 % en 2017) pour protéger leur infrastructure de technologies de l'information et des communications. Cependant, l'absence d'utilisation d'autres techniques de cybersécurité peut encore faire en sorte que les entreprises soient vulnérables aux incidents de cybersécurité. Par exemple, alors que 37 % des entreprises ont déclaré qu'elles avaient utilisé des appareils intelligents connectés à Internet ou des appareils de l'Internet des objets (à l'exclusion des téléphones intelligents, des tablettes, des ordinateurs portatifs et des ordinateurs de bureau) en 2019, 17 % des entreprises utilisant ces appareils en ont évalué la sécurité. La plupart des entreprises (65 %) ont aussi indiqué qu'elles n'ont pas installé de mises à jour de sécurité pour leurs logiciels et leurs systèmes d'exploitation tous les mois ou plus fréquemment.

En 2019, 44 % des entreprises ont déclaré qu'elles étaient tenues de mettre en œuvre des mesures de cybersécurité par des fournisseurs, des clients, des partenaires ou des organismes de réglementation, ou de respecter les exigences de normes ou de programmes de certification en matière de cybersécurité. Les secteurs industriels ayant le plus souvent déclaré être tenus de mettre en œuvre des mesures de cybersécurité étaient le secteur de la finance et des assurances (70 %), celui de l'industrie de l'information et de l'industrie culturelle (60 %) et celui des services publics (57 %).

Les trois cinquièmes des entreprises canadiennes ont des employés qui s'occupent régulièrement de tâches liées à la cybersécurité

En 2019, 60 % des entreprises canadiennes avaient au moins un employé qui s'occupait de tâches liées à la cybersécurité dans le cadre de ses responsabilités habituelles. Presque toutes les grandes entreprises (85 %) avaient au moins un employé avec cette fonction, alors qu'un moins grand nombre de moyennes entreprises (67 %) et de petites entreprises (58 %) ont déclaré avoir ce type d'employé.

Parmi les 35 % des entreprises ayant déclaré ne pas avoir d'employé qui s'occupait de tâches liées à la cybersécurité dans le cadre de ses responsabilités habituelles en 2019, 48 % ont indiqué que l'une des raisons principales pour lesquelles elles n'avaient pas ce type d'employé était que la cybersécurité ne représentait pas un risque assez élevé pour leur entreprise, tandis que 47 % ont indiqué qu'elles faisaient appel à des experts-conseils ou à des entrepreneurs pour surveiller la cybersécurité.

Portail de statistiques sur l'économie et la société numériques

Visitez le [Portail de 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.

Note aux lecteurs

Les données de cette enquête ont été recueillies de janvier à mars 2020. La population cible comprend les entreprises ayant des activités au Canada et comptant 10 employés ou plus, dans la plupart des secteurs économiques, à l'exception des administrations publiques. La taille de l'échantillon final était de 12 274 entreprises, et le taux de réponse, de 76 %.

Les questions d'enquête posées aux répondants portaient sur l'année de référence 2019 exclusivement; par conséquent, les répercussions de la pandémie de COVID-19 ne paraissent pas dans les résultats de cette enquête.

Les chiffres relatifs aux coûts totaux et moyens publiés pour le cycle de 2019 de cette enquête ne doivent pas être comparés avec ceux qui ont été publiés pour le cycle de 2017, étant donné que des changements ont été apportés à la méthodologie d'imputation. Les répondants à cette enquête ont indiqué que certains coûts liés à la cybersécurité sont difficiles à déclarer, car ils ne peuvent pas être facilement dissociés des dépenses générales pour la technologie et la gestion de l'information. Les chiffres relatifs aux coûts publiés pour l'enquête de 2017 comprenaient quelques ajustements de sorte à tenir compte de ces coûts liés à la cybersécurité que les répondants ont eu de la difficulté à déclarer. Après avoir consulté des spécialistes du domaine, il a été déterminé que le retrait de ces ajustements aux chiffres relatifs aux coûts de 2019 donnerait des données plus faciles à interpréter et à utiliser par les utilisateurs de données.

Les chiffres relatifs aux coûts moyens calculés pour le cycle de 2019 de cette enquête ne devraient pas non plus être comparés avec ceux qui ont été publiés pour le cycle de 2017, car les réponses de 0 \$ ont été exclues des calculs en 2017 et incluses dans ceux de 2019.

Les pourcentages publiés dans cet article représentent un pourcentage des entreprises.

On a seulement demandé aux entreprises de signaler les incidents qui les touchaient. Par conséquent, les incidents que les entreprises jugent sans effet ne sont pas compris dans ces données.

Tableaux disponibles : [22-10-0001-01](#), [22-10-0056-01](#), [22-10-0076-01](#), [22-10-0078-01](#) et [22-10-0128-01](#) à [22-10-0133-01](#) .

Définitions, source de données et méthodes : numéro d'enquête [5244](#).

Pour obtenir plus de renseignements ou pour en savoir davantage sur les concepts, les méthodes et la qualité des données, communiquez avec nous au 514-283-8300 ou composez sans frais le 1-800-263-1136 (STATCAN.infostats-infostats.STATCAN@canada.ca), ou communiquez avec les Relations avec les médias au 613-951-4636 (STATCAN.mediahotline-ligneinfomedias.STATCAN@canada.ca).