Impact of cybercrime on Canadian businesses, 2021

Released at 8:30 a.m. Eastern time in The Daily, Tuesday, October 18, 2022

Cyber Security and Cybercrime in 2021

The COVID-19 pandemic has highlighted the utility of digital technology use among Canadian businesses. Since the onset of the pandemic, work and business transactions have increasingly been conducted virtually rather than in-person, and along with this increase comes increased awareness and increased concerns about privacy, data protection and cyber security.

Most Canadian businesses have recognized this and have taken appropriate steps to ensure that they are protected. The Canadian Survey of Cyber Security and Cybercrime measures these precautions and policies put in place by Canadian businesses and shows how cybercrime incidents can impact businesses operations.

This release coincides with Cyber Security Awareness Month, which is an internationally recognized campaign held each October to inform the public of the importance of cyber security.

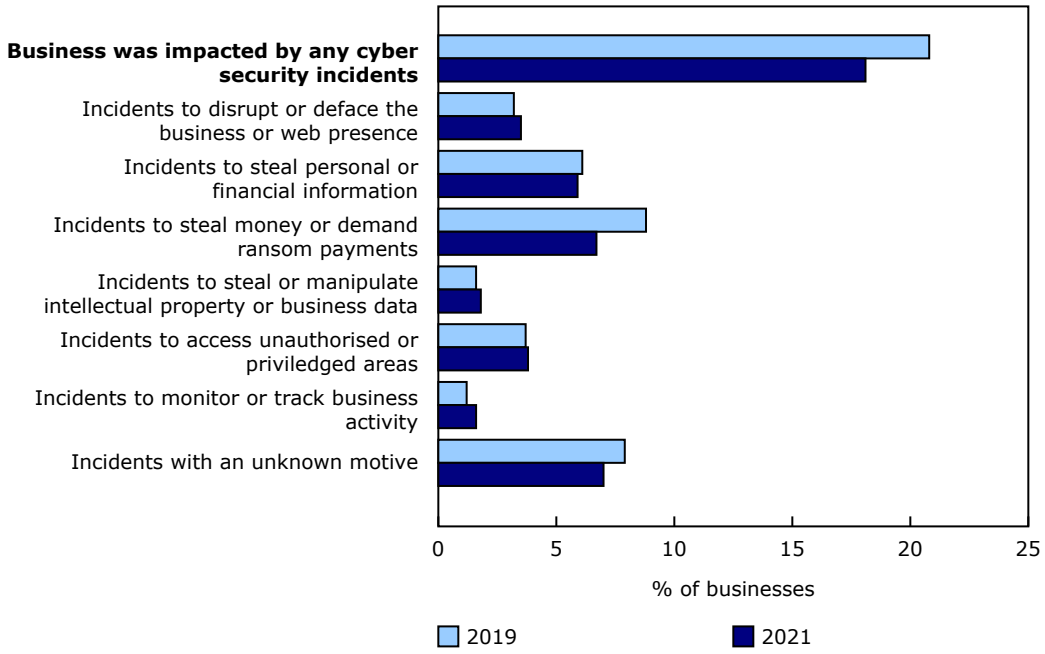
Just under one-fifth of Canadian businesses were impacted by cyber security incidents in 2021

A cyber security incident can impact businesses in different ways, such as by threatening the privacy and security of their customers' information, monetary losses, reputational damages, etc. In 2021, just under one-fifth (18%) of Canadian businesses were impacted by cyber security incidents, compared with 21% of Canadian businesses in both 2019 and 2017 that were impacted. This varied significantly by business size, with 16% of small businesses (10 to 49 employees), 25% of medium businesses (50 to 249 employees), and 37% of large businesses (250 or more employees) reporting being impacted by cyber security incidents in 2021.

The most common types of cyber security incidents identified by business in 2021 were incidents to steal money or demand ransom payments (7%) and incidents to steal personal or financial data (6%). More than one-third (39%) of Canadian businesses impacted by cyber security incidents indicated that there was no clear motive.

While most impacted businesses identified external parties (61%) as the perpetrator of cyber security incidents, 38% of impacted businesses could not identify the perpetrator. Other perpetrators identified were internal parties (5%) and known third parties (6%), like a supplier or customer.

Chart 1
Types of cyber security incidents that impacted businesses, Canada



Source(s): Canadian Survey of Cyber Security and Cybercrime (5244).

Canadian businesses reported spending over $10 billion on cyber security in 2021

The percentage of businesses that reported spending some money to detect or prevent cyber security incidents remained relatively the same in 2021 (61%) compared with 2019 (62%). However, the amount of money Canadian businesses spent to detect or prevent cyber security incidents increased by roughly $2.8 billion in 2021 to $9.7 billion when compared with 2019. Large businesses contributed to just under half of the total ($4.4 billion), followed by small businesses ($2.9 billion) and medium businesses ($2.4 billion).

Among the roughly one in five (18%) businesses that were impacted by a cyber security incident, about 40% experienced downtime as a result, with an average downtime duration of 36 hours. Other commonly reported impacts included additional time that was required by employees to complete their day-to-day work (21%), prevention of employees from carrying out their day-to-day work (18%), and loss of revenue (14%).

Canadian businesses that were impacted by a cyber security incident spent a total of slightly over 600 million dollars to recover, an increase of roughly 200 million dollars from 2019. This increase was driven by higher amounts spent amongst impacted businesses, as a smaller percentage of businesses in 2021 had expenses related to recovering from cyber security incidents compared with 2019, with 10% reporting expenses in 2019 and 7% reporting expenses in 2021.

Impacted businesses spend more to prevent and detect cyber security incidents

Canadian businesses that identified being impacted by cyber security incidents spent more money to prevent and detect incidents were more likely to employ dedicated cyber security employees, and were more concerned about cyber security incidents.

In 2021, businesses reporting that they were 'extremely concerned' or 'very concerned' about cyber security incidents spent significantly more on average (nearly $110,000 more) than businesses reporting they were 'slightly concerned' or 'not at all concerned' about cyber security incidents. Businesses reporting that they were 'extremely concerned' or 'very concerned' were also more likely to have reported an incident to police services (13% compared with 10%).

Additionally, businesses that were impacted by cyber security incidents spent more money on average ($113,000) to prevent or detect them than those that were not impacted ($39,000). Small businesses that were impacted spent 120% more than their counterparts who were not impacted, impacted medium businesses spent 39% more, and impacted large businesses spent 75% more.

Table 1
Average amount paid to prevent and/or detect cyber incidents, by businesses size, dollars

	Business was impacted by cyber incident	Business was not impacted by cyber incident
Small size businesses	35,000	16,000
Medium size businesses	104,000	75,000
Large size businesses	1,360,000	800,000
All business sizes	113,000	39,000

Note(s): Small size businesses: from 10 to 49 employees; medium size businesses: from 49 to 249 employees; large size businesses: more than 250 employees.
Source(s): Canadian Survey of Cyber Security and Cybercrime (**5244**).

Furthermore, businesses that were impacted by a cyber security incident were more likely to have reported having at least one cyber security employee compared with those that did not report an incident (79% compared with 57%). Businesses with at least one cyber security employee also reported a higher average downtime duration, with an average downtime duration of 38 hours compared with 28 hours for those with no employees.

There are two probable explanations for these observations. Firstly, businesses that were impacted by incidents are investing in preventive measures to avoid future negative impacts (e.g., hiring dedicated cyber security employees). Secondly, businesses that already invested more heavily in preparing for cyber security threats are in better position to detect and report them (e.g., businesses with a cyber security employee are more likely to be able to detect an incident compared with a business with no cyber security employees).

Canadian businesses are implementing formal policies for cyber security

In addition to increases in prevention and detection expenses, many Canadian businesses are implementing policies and procedures to mitigate risks. For example, over 6 in 10 Canadian businesses (61%) that designated at least one employee with responsibility for overseeing cyber security risks and threats, almost 4 in 10 Canadian businesses (38%) that had a consultant or contractor to manage cyber security risks and threats and almost one-third (29%) of Canadian businesses that had monthly or more frequent patching or updating of operating systems for security reasons.

Another risk management agreement for many businesses was cyber risk insurance, of which 16% of Canadian businesses had, down from 17% in 2019. For those with cyber risk insurance, their policies covered items such as direct losses from an attack or intrusion (84%), restoration expenses for software, hardware, and electronic data (75%), and businesses interruption and reputational losses (73%). Amongst Canadian businesses with cyber risk insurance that were impacted by cyber security incidents, 88% did not make a claim for the incident, 8% successfully made a claim against the insurance, and 2% attempted to make a claim but were unsuccessful.

Overall, 1 in 10 businesses impacted by ransomware, and fewer made ransom payments

As ransomware becomes more known and utilized by attackers, in 2021, 11% of Canadian businesses that were impacted by a cyber security incident were impacted by ransomware. Among these businesses, a large proportion (82%) did not pay the ransom, while a smaller proportion (18%) reported making a ransom payment, with 1% paying more than $500,000. In addition, among those that made a ransom payment, 14% of them did so with cryptocurrency.

To resolve a ransomware attack, 6 in 10 (60%) businesses impacted by ransomware used an external information technology (IT) consultant or contractor, 14% worked with other external parties, and 13% went through their cyber risk insurance provider.

Fewer businesses reported incidents to police services in 2021

Overall, 1 in 10 (10%) businesses that were impacted by a cyber security incident reported the incident to police services, a decrease of roughly 2 percentage points from 2019, when 12% of businesses reported incidents to police services. Small, medium, and large businesses all saw a decrease in reporting to police services from 2019 to 2021.

Businesses that reported incidents to police were also three times more likely to have reported being impacted by an incident involving theft or manipulation of intellectual property or business data (26% compared with 8%), twice as likely to have reported being impacted by an incident involving theft of money or demands for a ransom payment (66% compared with 34%), and were twice as likely to have reported being impacted by an incident that disrupted or defaced the business or web presence (38% compared with 17%), when compared with those that did not report incidents to police services.

In addition, businesses that reported incidents to police services reported an average cost of $53,500 to recover from cyber security incidents, compared with $14,000 for those that did not report the incident to police services.

Of those that did not report cyber security incidents to police services, the main reasons for not doing so were that the incidents were resolved internally (43%), incidents were resolved through an IT consultant or contractor (30%), or that the incidents were minor and not important enough for business (29%).

Note to readers

Data for this survey were collected from January to March 2022. The target population included enterprises with Canadian operations and 10 or more employees, across most economic sectors, except for public administration. The final sample size was 12,216 enterprises and the response rate is 74%.

The total and average cost figures published for the 2019 and 2021 iterations of this survey should not be compared to those published for the 2017 iteration due to changes in the imputation methodology. Respondents for this survey have indicated that some cyber security costs are difficult to report since they cannot be easily separated from general information technology and management expenses. The cost figures published for the 2017 survey included some adjustments to account for these cyber security costs respondents had difficulty reporting. After consulting with subject matter experts, it was determined that removing these adjustments from the 2019 and 2021 cost figures would result in data that are easier for data users to interpret and use.

The average cost figures calculated for the 2019 and 2021 iterations of this survey should also not be compared to those published for the 2017 iteration since responses of $0 were excluded in the calculations in 2017 and included in 2019 and 2021.

Businesses were only asked to report on incidents that impacted them. Therefore, incidents that businesses deemed not to be impactful are not captured in these data.

Available tables: 22-10-0001-01, 22-10-0056-01, 22-10-0076-01, 22-10-0078-01 and 22-10-0128-01 to 22-10-0133-01 .

Definitions, data sources and methods: survey number 5244.

For more information, or to enquire about the concepts, methods or data quality of this release, contact us (toll-free 1-800-263-1136; 514-283-8300; **infostats@statcan.gc.ca**) or Media Relations (**statcan.mediahotline-ligneinfomedias.statcan@statcan.gc.ca**).