

Impact of cybercrime on Canadian businesses, 2023

Released at 8:30 a.m. Eastern time in *The Daily*, Monday, October 21, 2024

While digitalization and a growing online presence have created many new opportunities for Canadian businesses, they have also exposed businesses to new risks regarding privacy, data protection and cyber security. In 2023, total spending on recovery from cyber security incidents doubled from 2021, demonstrating the growing importance of cyber preparedness.

Since 2017, the Canadian Survey of Cyber Security and Cybercrime (CSCSC) has collected data on the policies and measures put in place by Canadian businesses to manage cyber security and investigated how cyber security incidents impact their operations.

The release of 2023 data from the CSCSC 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.

Proportion of businesses impacted by cyber security incidents continues to decline

In 2023, about 1 in 6 (16%) Canadian businesses were impacted by cyber security incidents. The proportion of businesses impacted by cyber security incidents has been declining since 2019, with 21% of businesses being impacted that year and 18% in 2021.

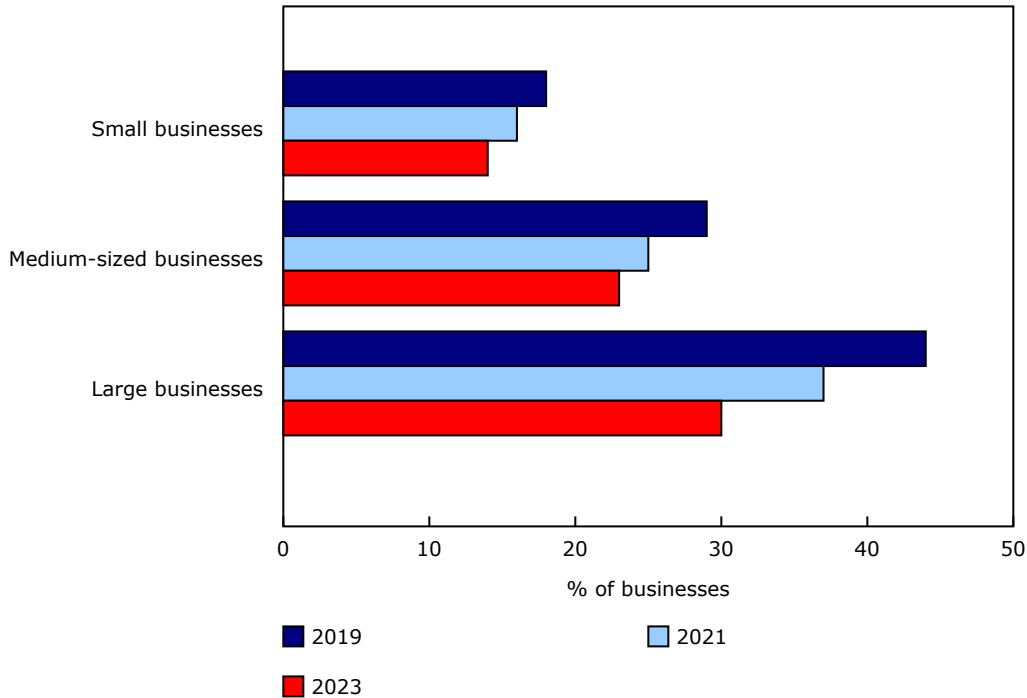
This trend is consistent with the United Kingdom's [Cyber Security Breaches Survey](#), which found that the proportion of businesses impacted by cyber breaches or attacks also decreased in the United Kingdom from 2019 (18%) to 2022 (12%).

In Canada, large businesses (-7 percentage points) reported the largest drop in 2023 but remained the most likely to be impacted (30%).

In contrast to the trend observed for Canadian businesses, the [Canadian Internet Use Survey](#) found that the proportion of Canadian individuals aged 15 and older experiencing cyber security incidents has been rising since 2018. Over two-thirds (70%) of Canadians experienced a cyber security incident in 2022, up from 2020 (58%) and 2018 (52%).



Chart 1
Businesses impacted by cyber security incidents, Canada, 2019 to 2023



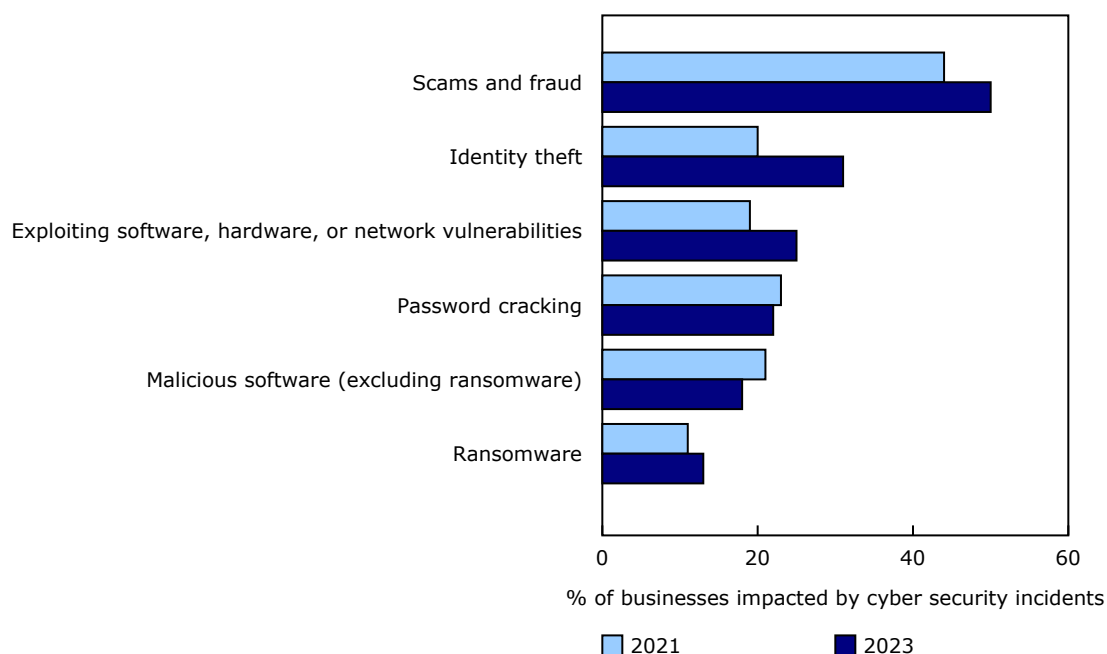
Source(s): Table 22-10-0076-01.

Identity theft, scams and fraud, and ransomware impacting a larger proportion of businesses

While the proportion of Canadian businesses impacted by cyber security incidents declined overall in 2023, certain methods of attack were significantly more prevalent. Identity theft had the largest change, with just under one-third (31%) of impacted businesses experiencing incidents using that method. This was an 11-percentage point increase from 2021. The next largest increase was for scams and fraud (50%), up by 6 percentage points from 2021. Scams and fraud remained the most commonly used method for cyber security incidents.

In 2023, over 1 in 8 (13%) impacted businesses reported experiencing ransomware attacks, up from 11% in 2021. The majority of ransomware victims did not make a ransom payment (88%). Of those that did indicate making a ransom payment, the majority (84%) paid less than \$10,000, while 4% paid more than \$500,000.

Chart 2
Methods most commonly used for cyber security incidents, Canada, 2021 and 2023



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

Spending on recovery from cyber security incidents doubles, while preventative spending is stable

Total spending on recovery from cyber security incidents also increased in 2023, doubling from approximately \$600 million in 2021 to \$1.2 billion in 2023. This followed an increase of about \$200 million from 2019 to 2021.

Large businesses accounted for almost half of total spending on recovery from cyber security incidents in 2023 (about \$500 million), while medium-sized and small businesses each spent approximately \$300 million. The trend of increasing recovery spending may indicate that, although a lower percentage of businesses fell victim to cyber security incidents, the financial consequences of being hit by incidents are becoming more severe.

In contrast to recovery spending, total spending on prevention and detection of cyber security incidents rose at a slower pace, increasing from \$9.7 billion in 2021 to \$11.0 billion in 2023. Large businesses accounted for almost half of the total in 2023 (\$4.8 billion), followed by medium-sized (\$3.6 billion) and small (\$2.6 billion) businesses. The proportion of businesses that reported spending money to prevent or detect cyber security incidents decreased from 61% in 2021 to 56% in 2023.

The largest cyber security cost for businesses in 2023 was employee salary related to prevention or detection (\$3.8 billion). Half of businesses (50%) reported having cyber security employees in 2023, down from 61% in 2021.

The most reported reason for not having cyber security employees was that the business used consultants or contractors to monitor cyber security (47%). Consultant or contractor expenses were the third-largest prevention or detection cost (\$1.9 billion), following cyber security software costs (\$2.9 billion).

In addition to hiring expenses, just over one-fifth of businesses (22%) provided formal training to develop or upgrade the cyber security skills of their non-information technology employees in 2023. The cost of providing training to employees, suppliers, customers or partners totalled over \$300 million.

Usage of written policies remains at 2021 levels, while usage of cyber risk insurance is up

The COVID-19 pandemic forced many Canadian businesses to move more of their operations online, requiring them to also adopt additional cyber security precautions. Many of these precautions continue to be used even as pandemic-related restrictions have been lifted.

Just over 1 in 4 Canadian businesses (26%) had written policies for cyber security in place in 2023, the same proportion as in 2021 (26%). Meanwhile, 22% of businesses had cyber risk insurance in 2023, up 6 percentage points from 2021 (16%). For those with cyber risk insurance, their policies covered items such as direct losses from an incident (53%), restoration expenses for software, hardware, and electronic data (44%), business interruptions (39%) and financial losses (38%).

The proportion of businesses conducting any activities to identify cyber security risks (59% in 2023) has also been relatively stable since 2019 (60%). The most common cyber security activity in 2023 was monitoring network and business systems (46%), followed by monitoring insider threat risk behaviours (22%).

Reporting of cyber security incidents to police services increases in 2023

About 1 in 8 (13%) Canadian businesses impacted by cyber security incidents reported incidents to police services in 2023, up 3 percentage points from 2021 (10%). Large businesses were the most likely to report incidents (16%), followed by medium-sized (15%) and small (12%) businesses. The leading types of incidents reported were incidents to steal money or demand ransom payment (56% of businesses reporting incidents to police services), followed by incidents to steal personal or financial information (33%).

Among impacted businesses that did not report all incidents to police services, the primary reasons given for not reporting were that the incidents were resolved internally (55%), were too minor (35%), or were resolved through information technology consultants or contractors (31%).

Digital economy and society statistics portal and publications

For more information on the digital economy and society, visit the [Digital economy and society statistics](#) portal and the [Digital Insights](#) publication, which bring together a variety of data from across Statistics Canada and other sources to provide statistics, analysis and interactive tools related to the digital economy and society in Canada.

Did you know we have a mobile app?

Download our mobile app and get timely access to data at your fingertips! The [StatsCAN](#) app is available for free on the [App Store](#) and on [Google Play](#).

Note to readers

Data for the 2023 Canadian Survey of Cyber Security and Cybercrime (CSCSC) were collected from January to March 2024. Respondents were asked to only report activities that occurred in 2023.

The target population of the 2023 CSCSC included enterprises with Canadian operations and 10 or more employees, across most economic sectors, except for public administration. The final sample size was 12,462 enterprises and the response rate was 71%.

The business size categories presented in this release are based on the enterprise's number of employees:

- Small businesses have 10 to 49 employees.
- Medium-sized businesses have 50 to 249 employees.
- Large businesses have 250 or more employees.

In 2023, the CSCSC's target population included approximately 5,000 large, 30,000 medium-sized and 170,000 small businesses.

For indicators related to cyber security incidents and their effects on business operations, businesses were only asked to report on incidents that impacted them. Therefore, incidents that businesses deemed not impactful are not captured in these indicators. Since non-impactful incidents are not measured, the figures presented in this release may not accurately reflect the total number of cyber-attacks in Canada.

In this release, comparisons are made with the United Kingdom's [Cyber Security Breaches Survey](#) due to its methodological similarity to the CSCSC. In the Cyber Security Breaches Survey, businesses were first asked if they experienced any cyber breaches or attacks and then asked a follow-up question about whether the breaches or attacks were impactful. For more accurate comparison with the CSCSC, the percentage of United Kingdom businesses impacted by breaches or attacks was mathematically derived from those two survey questions.

The "Password cracking" category in chart 2 was reworded in 2023. In previous survey iterations, the category was "Hacking or password cracking." This change may have had a small impact on the observed trends.

Cost figures published for the 2017 CSCSC are not comparable with later iterations due to changes in the data imputation strategy and the aggregate calculation methodology.

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).