Catalogue no. 22200001
ISBN 978-0-660-48648-2

Digital Insights

The changing landscape of cyber security following the COVID-19 pandemic

by Gabrielle Asselin and Howard Bilodeau

Release date: July 11, 2023

Statistics Canada Statistique Canada

Canada

How to obtain more information

For information about this product or the wide range of services and data available from Statistics Canada, visit our website, www.statcan.gc.ca.

You can also contact us by

Email at infostats@statcan.gc.ca

Telephone, from Monday to Friday, 8:30 a.m. to 4:30 p.m., at the following numbers:

- Statistical Information Service 1-800-263-1136
- National telecommunications device for the hearing impaired 1-800-363-7629
- Fax line 1-514-283-9350

Standards of service to the public

Statistics Canada is committed to serving its clients in a prompt, reliable and courteous manner. To this end, Statistics Canada has developed standards of service that its employees observe. To obtain a copy of these service standards, please contact Statistics Canada toll-free at 1-800-263-1136. The service standards are also published on www.statcan.gc.ca under "Contact us" > "Standards of service to the public."

Note of appreciation

Canada owes the success of its statistical system to a long-standing partnership between Statistics Canada, the citizens of Canada, its businesses, governments and other institutions. Accurate and timely statistical information could not be produced without their continued co-operation and goodwill.

Published by authority of the Minister responsible for Statistics Canada

An HTML version is also available.

Cette publication est aussi disponible en français.

The changing landscape of cyber security following the COVID-19 pandemic

by **Gabrielle Asselin** and **Howard Bilodeau**

Societal changes accelerated by the COVID-19 pandemic have had an unprecedented impact on the operations of Canadian businesses, motivating many to change their business models and begin using the Internet and other technologies in new ways. According to the Survey of Digital Technology and Internet Use, a third (33%) of Canadian businesses received orders or made sales of goods and services over the Internet in 2021, up from 25% before the pandemic in 2019. More businesses also reported offering employees the option to telework in 2021 compared with 2019 (+14 percentage points).[1]

While a growing online presence has created new opportunities for many businesses, it has also exposed them to new risks regarding privacy, data protection and cyber security. Many of the types of crime in the news in 2021, including cybercrime, fraud and counterfeiting, were not new, but rather existing types of crime taking advantage of technological developments to improve on techniques.[2] This article examines how Canadian businesses are adapting to cyber security threats in the aftermath of the pandemic by leveraging data from the Canadian Survey of Cyber Security and Cybercrime (CSCSC).[3]

Canadian businesses are taking more cyber precautions

In 2021, 26% of Canadian businesses had written policies in place related to cyber security, an increase of at least four percentage points since 2019.[4] This demonstrates that businesses are becoming increasingly aware of the threat posed by cyber security incidents.

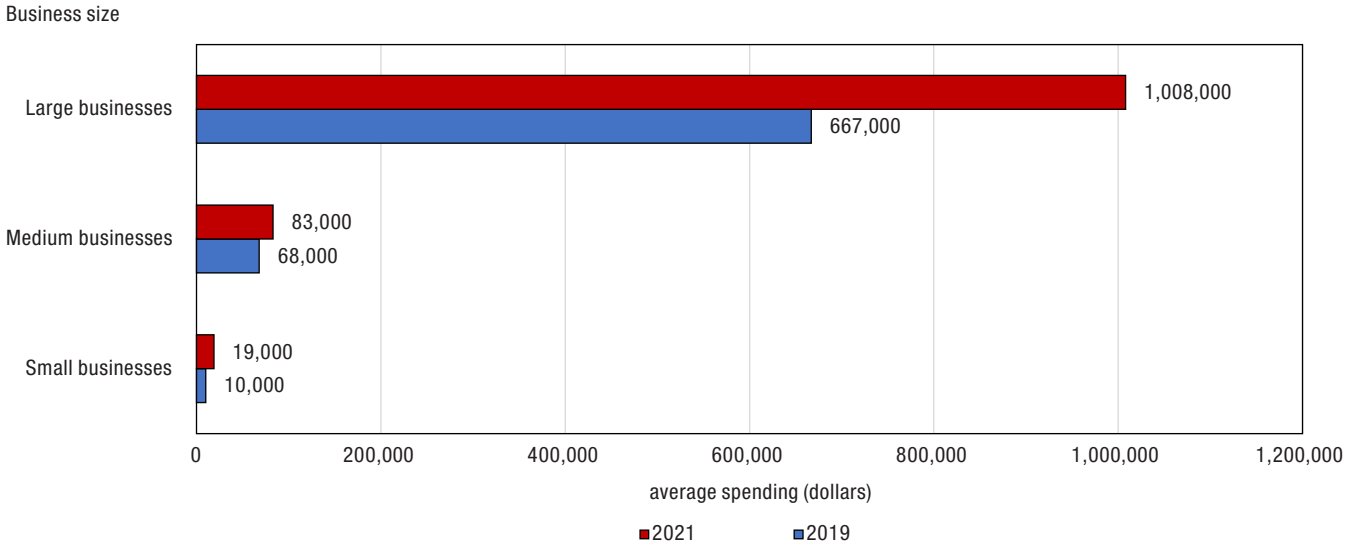
Businesses also demonstrated growing cyber-awareness in other ways; for example, the proportion of businesses conducting activities to identify cyber security risks on a scheduled basis increased by five percentage points to 39% in 2021. Data from the Canadian Survey on Business Conditions for the second quarter of 2022 also showed that one fifth (21%) of Canadian establishments plan to take new or additional cyber security actions over the next twelve months.[5]

Canadian businesses are spending more on cyber security prevention and detection

The apparent increase in cyber security awareness among Canadian businesses was also reflected in their cyber security spending. In 2021, the average spending on prevention and detection of cyber security incidents was $52,000, a substantial 46% increase from 2019 which far outpaced the inflation rate over the same period (+4%).[6] In 2021, large businesses spent about $340,000 more on prevention and detection of cyber security incidents than they did in 2019, whereas small businesses spent about $9,000 more. However, the increase in cyber security awareness may not be occurring evenly throughout the economy; four in ten businesses still did not report any direct expenditures on cyber security in 2021, a figure that has not changed since 2019.

1. An article highlighting results for 2021 from the Survey of Digital Technology and Internet Use was released in *The Daily* on September 13, 2022. A companion article using data from the same survey titled "Changes in the e-commerce strategies of Canadian businesses during the COVID-19 pandemic" was released on November 29, 2022.
2. Data from the European Commission: Guide to statistics in European Commission development cooperation – 2021 edition – Volume 2: Population and social statistics.
3. Results for 2021 from the Canadian Survey of Cyber Security and Cybercrime were released in *The Daily* on October 18, 2022. This article expands upon the trends highlighted in the article in *The Daily*.
4. Statistics for written policies related to cyber security were derived from question 12 on the 2019 and 2021 iterations of the CSCSC. Some of the response categories for this question were reworded or split in 2021, and a new category for "other type of written policy related to cyber security" was added. Excluding the new "other" category, the increase in adoption of written policies from 2019 to 2021 was four percentage points.
5. Data from the Canadian Survey on Business Conditions: Business' or organization's plans to take any new or additional cybersecurity actions over the next 12 months, second quarter of 2022. The Canadian Survey on Business Conditions surveys establishments, whereas the CSCSC surveys enterprises. One enterprise may have multiple establishments, so comparisons between the two data sources should be made with caution.
6. Data from the annual average Consumer Price Index.

Chart 1
Average amount spent on cyber security incident prevention and detection, by business size, 2019 and 2021



Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime, 2019 and 2021.

Part of the motivation of some businesses to invest more in cyber defenses and policies may be the parallel awareness among consumers of the potential risks of sharing their personal information when shopping online. The 2020 Canadian Internet Use Survey found that one-quarter (25%) of Canadian individuals were very or extremely concerned about cyber security or privacy threats when using online shopping sites or applications.[7] Similarly, in the CSCSC 2021, protecting personal information was the most common reason businesses gave for spending time or money on cyber security, with two-thirds (66%) selecting that response.

Despite businesses demonstrating growing cyber-awareness in some areas of their operations, the trend was not universal; the proportion of businesses that had dedicated cyber security employees remained largely unchanged from 2019 (60%) to 2021 (61%), and only slightly more businesses provided formal training to develop or upgrade the cyber security skills of their non-information technology employees in 2021 (+3 percentage points). Human error has long been known as a major source of cyber security incidents, so increasing the cyber security knowledge of all employees can play an important role in improving organizational cyber resilience.[8]

Fewer Canadian businesses were impacted by cyber security incidents in 2021 but the reported costs of incidents were higher

Slightly fewer Canadian businesses (18%) reported being impacted by a cyber security incident in 2021 than in 2019 (21%). This differed from the trend observed for Canadian individuals in the 2020 Canadian Internet Use Survey, where the percentage of individuals impacted by cyber security incidents increased by six percentage points to 58% from 2018 to 2020.[9] These trends may reflect a change in the strategies of cyber criminals, but could also be the result of businesses having more tools at their disposal to identify and intercept malicious cyber activities when compared with individuals.

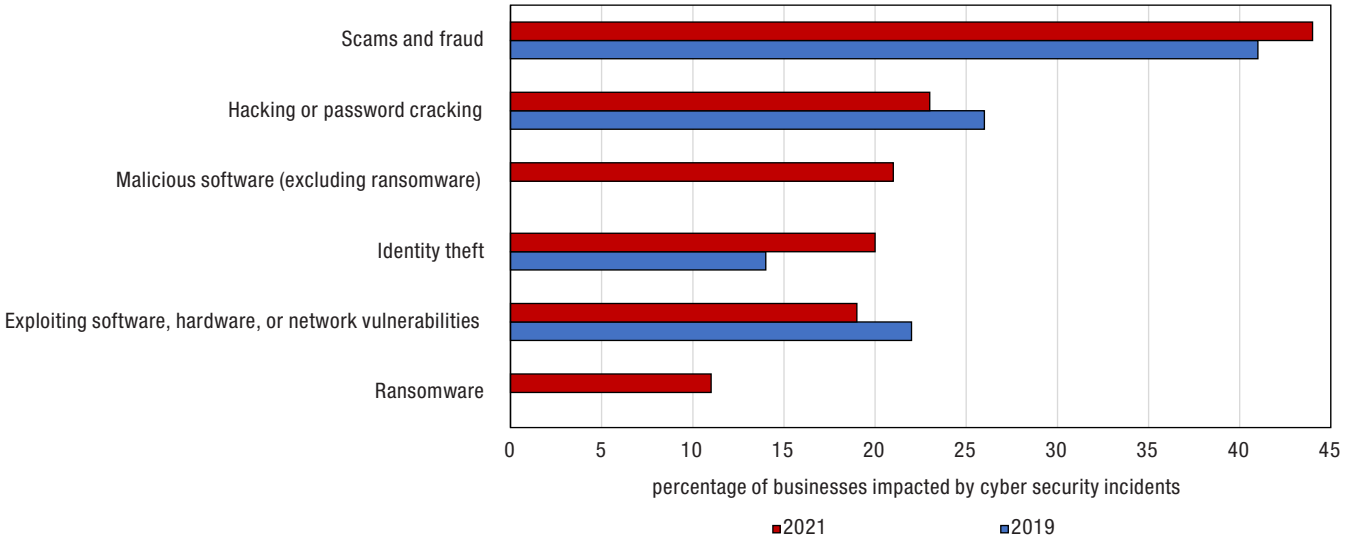
Although the previous sections presented evidence that businesses are becoming more cyber-aware, those that were impacted by cyber security incidents in 2021 faced worse financial consequences when compared with 2019. On average in 2021, businesses paid $19,000 to recover from cyber security incidents, $8,000 more than 2019 ($11,000). This increase was largely driven by a substantial rise in costs incurred by large businesses from 2019 ($73,000) to 2021 ($172,000).

7. Data from the Canadian Internet Use Survey: Level of concern about security and privacy threats when using applications or digital technologies.
8. Results from the World Economic Forum's Global Risks Report 2022.
9. Data from the Canadian Internet Use Survey: Canadian Internet Use Survey, 2020.

Businesses that had written policies in place related cyber security were also found to be more likely to be impacted by cyber security incidents (25%) than those without policies (16%) in 2021. This finding could be the result of cyber-aware businesses being better positioned to notice cyber security incidents compared with those that don't have monitoring procedures in place. Businesses that are more frequently targeted by cyber security incidents may also be more likely to adopt written policies related cyber security. Additionally, although businesses with written policies were impacted by cyber security incidents at a higher rate than those without, there were still more businesses without written policies impacted by incidents (22,000) than ones with written policies (12,000) in 2021. This was due, in part, to the fact that 74% of businesses did not have written policies in place.

Among businesses impacted by cyber security incidents, identity theft had the largest increase in 2021 compared with 2019 (up six percentage points to 20%). Conversely, the proportions of businesses reporting being impacted by hacking or password cracking (-3 percentage points) and exploiting software, hardware, or network vulnerabilities (-3 percentage points) decreased in 2021. Measured for the first time in 2021 as its own category, 11% of Canadian businesses that were impacted by a cyber security incident reported being impacted by ransomware.[10]

Chart 2
Methods used for cyber security incidents, businesses impacted by cyber security incidents, 2019 and 2021



Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime, 2019 and 2021.

Digital economy and society statistics portal

Visit the Digital economy and society statistics portal to find data, publications, and interactive tools related to the digital economy and society in one convenient location.

Methodology

Data in this article are from the Canadian Survey of Cyber Security and Cybercrime (CSCSC), unless otherwise indicated.

Data for the 2021 iteration of the CSCSC were collected from January to March, 2022. The target population of this survey was derived from Statistics Canada's Business Register (BR). The BR is an information database on the Canadian business population and serves as a frame for all Statistics Canada business surveys. It is a structured list of businesses engaged in the production of goods and services in Canada. This survey covers enterprises

10. Prior to the 2021 iteration of the Canadian Survey of Cyber Security and Cybercrime, ransomware was contained within the category of malicious software.

operating in Canada in almost all industrial sectors. Businesses with less than 10 employees were excluded from the sample. The final sample size was 12,158 enterprises and the response rate was 65%.

To create the sample for this survey, enterprises were stratified by industry and size categories. The size category is based on the number of employees of the enterprise. Three size categories were built: small (10-49 employees), medium (50-249 employees) and large (250 or more employees).

Percentages published in this article represent a percentage of businesses, unless otherwise indicated. Survey weights were used in all calculations to ensure the results were reflective of the target population. Percentage point changes from the CSCSC are only given for proportions with a quality of "A" (standard error up to 2.5%).

Acknowledgments

The CSCSC is conducted on behalf of Public Safety Canada. The authors would like to thank colleagues from Public Safety Canada for their advice and comments on an earlier version of this paper.

External references

European Commission (2021). Guide to statistics in European Commission development cooperation, Volume 2: Social statistics. Retrieved March 16, 2023.

World Economic Forum (2022). The Global Risks Report 2022, 17th Edition, Insight Report. Retrieved March 16, 2023.