RESEARCH SNAPSHOT
FEBRUARY 2021

CANADIAN FEDERATION OF INDEPENDENT BUSINESS
In business for your business

CYBERFRAUD IN SMALL BUSINESS

How small businesses are coping with cyberattacks during the pandemic

Andreea Bourgeois, Senior Analyst

The pandemic has had, and is still having, a huge impact on small businesses. For some businesses, the use of technology has helped to mitigate the negative effects of government mandated closures and other public health restrictions. However, as businesses increasingly turned to technology and remote working to cope with the pandemic, they have opened themselves up to more cyberattacks. Canadian Federation of Independent Business (CFIB) research found that one in 20 Canadian small businesses have been the victim of cyberfraud in the past six months. CFIB estimates that, on average, a small business has invested an additional $6,700 in securing its IT systems to better protect their business during the pandemic.

What are cyberattacks against businesses?

A cyberattack is any attempt to damage or hack someone's computer system, steal the information on it, or steal money from someone using the internet. Examples of cyberattacks include malicious software, such as spyware and malware; email scams and phishing; and supplier payments fraud, which are defined as tricks designed to make businesses wire money to a scammer's bank account thinking they are paying a supplier. In this report, cyberattacks and cyberfraud are used interchangeably.

Cyberattacks – a growing concern during the pandemic

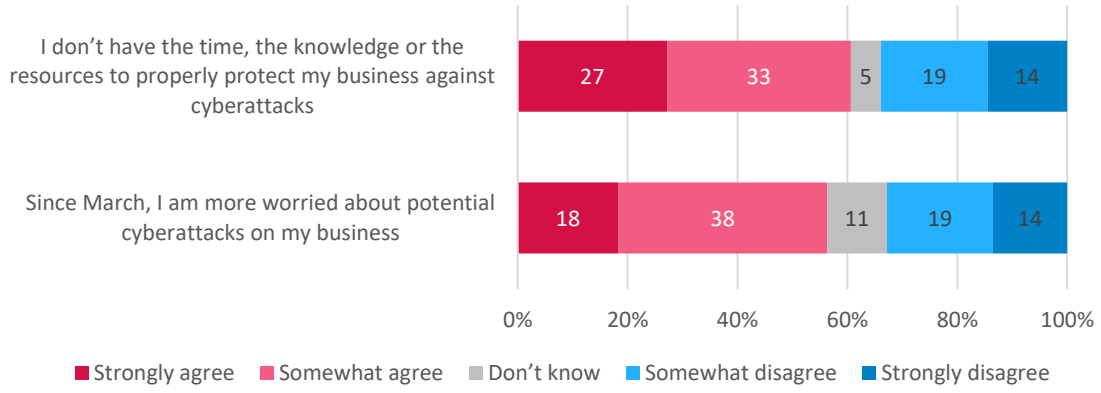
While there is some research on cyberfraud against businesses, it focuses mostly on larger firms and almost all is pre-pandemic.[1] The most recent data on cyberfraud from Statistics Canada looks only at firms with 10 or more employees. This report attempts to fill this gap by focusing on the types of cyberattacks smaller businesses have experienced and their impacts during the pandemic, specifically from March to October 2020. The report also provides an estimate of the financial cost of investing in technology to prevent cyberattacks – something many small businesses can ill afford during the pandemic.

There is no doubt that the pandemic has changed the business landscape in many ways. Governments mandated which businesses were deemed essential and this resulted in changes in how customers were served and payments were received. For some firms, the use of technology has mitigated the vast shutdowns mandated by governments, but it has also created new worries for entrepreneurs regarding the potential for cyberattacks. These can cause stress for the business owner, in addition to lost time, the loss of money, goods or services, or valuable information such as databases or banking information.

CFIB's survey found that 56 per cent of entrepreneurs are more worried about potential cyberattacks since March (see Figure 1). This was even more prevalent among small employers with employees who could work remotely with two-thirds expressing worry about the threat of cyberattacks. For many small businesses operating on tight margins, every dollar counts and they cannot afford to lose even more money due to cyberfraud. Two thirds of business owners reported they did not have the time, knowledge or resources to protect their business against cyberattacks.

Figure 1

To what extent you agree or disagree with the following statements about cyberattacks (per cent response)



1. Statistics Canada, The Daily, October 20, 2020. *About one-fifth of Canadian businesses were impacted by cyber security incidents in 2019. Results from a National Survey, January to March 2020,* Ottawa: Statistics Canada. Component of Statistics Canada catalogue no. 11-001-X. [PDF] Accessed on November 4, 2020: https://www150.statcan.gc.ca/n1/en/daily-quotidien/201020/dq201020a-eng.pdf?st=p-qG4DO2

Survey methodology

The Your Business and Cyberattacks Survey was conducted online from October 15th to the 29th with CFIB members from across the country. A total of 3,040 owners of small- and medium-sized businesses participated, which corresponds to an overall margin of error of ±1.8 per cent, 19 times out of 20. The survey questions and aggregate responses are available in Appendix A.

The effect of cyberfraud on small businesses during the pandemic

While about three quarters of Canadian small businesses did not experience any cyberattacks in the past six months, almost one sixth experienced attempted cyberattacks and one in 20 small businesses fell victim to cyberattacks (see Figure 2). By extrapolating to the entire economy, by size of business, and using the percentages of businesses who were victims of cyberfraud, it translates into about 61,000 businesses who fell prey to cyberattacks[2].

Figure 2

Which of the following applies to your business' experience with cyberattacks since March? (per cent response)

Cyberattacks cause much more than financial losses. The largest hidden costs of cyberattacks is the time needed to deal with the situation and the stress it brings onto the owner (see Figure 3). When a business is victimized, the owner must deal with the outcome of the cyberattack – which takes his or her time and focus away from productive business operations. Three quarters of respondents that were victims of a cyberfraud report loss of time, and almost two thirds report increased stress to deal with the cyberfraud. In addition, one in two victims reported financial losses as a direct result of cyberattacks since March. Losing money to

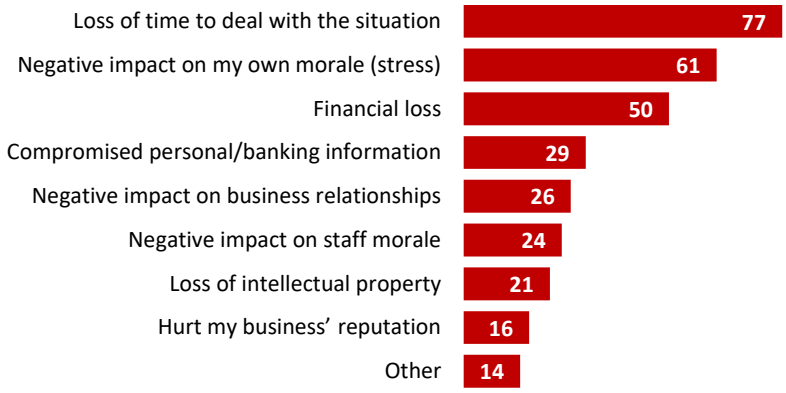
2. Source : Calculations done by CFIB by extrapolating survey data to the number of small and mid-sized businesses in Canada based on Canadian Business Counts, with employees, June 2020 (statcan.gc.ca), accessed on January 11, 2021.

cyberfraud on top of lower than normal revenues due to the pandemic makes an already difficult situation even tougher for a small firm.

Firms who allowed their employees to work remotely or made any changes to their online presence and operating in the construction, manufacturing, or wholesale sectors were twice as likely to be victims of cyberfraud (on average 10 per cent versus 5 per cent for the whole sample).

Figure 3

What impacts have cyberattacks had on you or your business since March? (per cent response)



Similar to CFIB's findings in its *2015 Fraud Survey*, businesses operating in the wholesale sector are most likely to experience cyberattacks. Wholesalers tend to have a larger number of different suppliers and types of customers, with many different ways of communicating with them. In addition to emails, technology is widely used for payments, orders, etc., so these businesses can be at higher risk for cyberattacks (see Table 1).

Businesses with 20 or more employees also tend to be more at risk for cyberattacks. Mid-sized businesses have more employees connected to a network or accepting and processing orders and payments; hence, more potential entry points for cyberattacks.

Table 1

Businesses that are most likely to be hit by cyberattacks: by size and by sector

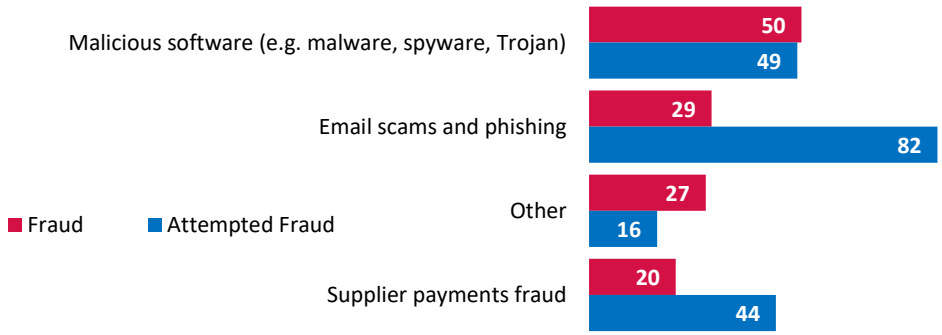
	Attempted cyberattack	Victim of cyberattack
By size	Businesses that have more than 20 employees	Businesses that have more than 20 employees
By sector	Businesses in manufacturing, wholesale, professional services, and enterprise and administration management sectors	Businesses in construction, manufacturing, wholesale, transportation, and enterprise and administration management sectors

Most common types of cyberattacks

Cyberattacks can occur in many ways. One way is the use of malicious software, such as malware, spyware and Trojan software. This is, by far, the most common type of cyberattack **causing a loss** for one in two victim firms (see Figure 4). Email scams and phishing are designed to trick business owners into providing sensitive information or transferring money. They are the most attempted types of fraud with 82 per cent of business owners reporting seeing them and about 30 percent falling victim. About one fifth of business owners fell victim to supplier payments fraud which is meant to trick businesses into wiring money to a scammer's bank account.

Figure 4

Types of attempted cyberattacks vs. types of cyberattacks that victimized small firms since March (per cent response)



Small businesses and cyberattacks prevention

Based on survey data, the average small business has spent $6,700[3] on additional investments in technology to protect their businesses during the pandemic. These investments can include upgrading to paid software from a previous free version, purchasing extra software to protect the network, paying for additional services from an external IT company, extra hours of work from the firm's own IT team or additional training provided to employees in matters of cybersecurity.

Despite the very challenging business circumstances since March, about one in three small businesses made some additional investments to protect their business from fraud (see Figure 5). Moreover, among those who invested in new or upgraded technology, they mostly invested in paid software, enhanced their own technology departments, or expanded external technology services they were already using.

3. See Appendix A for the exact survey question.

Data shows firms that have been a victim of past cyberattacks are more likely to invest in improved technology to prevent them from occurring in the future. Not surprisingly, firms that have made any changes in their online activities since March—such as developing a website, accepting payments, orders, or reservations online—were more likely to make additional investments in technology.

Regardless of the additional investments in protection against cyberattacks, what if one is successful? Unfortunately, there is little recourse available to the firm. However, cyber insurance can protect businesses from Internet-based risks such as data breaches.

Figure 5

Other than your typical IT investments, has your business made any additional investments to protect your IT systems since March? (per cent response)

What is cyber insurance?

Cyber insurance is insurance for businesses that covers liability arising from use of computers and computer networks, as from theft of private data, virus transmission, and trademark or copyright infringement.[4]

Cyber insurance coverage for cyber risks is relatively new and continually evolving.[5] This type of insurance can cover legal and civil damages, crisis management expenses, computer programming and electronic data restoration expenses, business interruption and additional expenses.

4. Cyber insurance." *Merriam-Webster.com Legal Dictionary*, Merriam-Webster, https://www.merriam-webster.com/legal/cyber%20insurance. Accessed Nov. 5, 2020

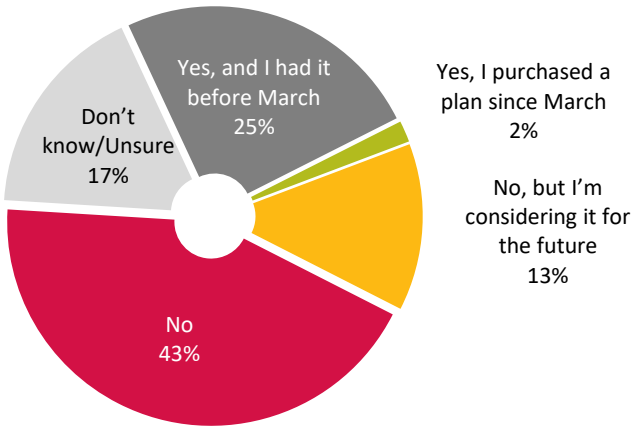
5. Insurance Bureau of Canada, Protect your organization from cyber crime (ibc.ca), accessed on Nov. 24, 2020.

Currently, almost 60 percent of businesses do not have cyber insurance, although 13 per cent are considering purchasing it in the near future (see Figure 6). About one quarter of businesses had cyber insurance even before March 2020[6], and a few firms purchased such an insurance policy despite the difficult economic conditions (2 per cent).

Businesses most interested in cyber insurance are those operating in the wholesale, finance, leasing and real estate, and professional service sectors. Those who have been a victim of past cyberattacks and those who have had to pivot to online sales or require employees to work remotely during the pandemic are also more likely to consider investing in cyber insurance.

Figure 6

Does your business have cyber insurance? (per cent response)



Conclusion

Many small firms, especially those who managed to find ways to provide their products and services online, have growing concerns about cyberfraud. During the pandemic, about 61,000 firms have been victims of cyberfraud, mostly those who tried to adjust rapidly and be more present online or allow their employees to work remotely, and the vast majority in wholesale, construction or manufacturing.

The losses and resulting costs of cyberattacks can be significant for small businesses and the chances of recovery of data or money are low. Small business owners have invested, on average, $6,700 in additional money to ensure their business is better protected and can survive during the pandemic.

With second waves of COVID-19 hitting many regions across the country and ongoing government-mandated shutdowns of businesses, technology will continue to play a greater role

6. CFIB, Cybersecurity Survey, Oct. 2019 – January 2020, 2,778 responses, Canada data, margin of error ±1.8 per cent, 19 times out of 20. Question 14 shows 28% respondents have cybersecurity.

in helping firms operate. The best ways for SMEs to protect themselves from cyberfraud is to be informed of the risks, invest in the right fraud prevention technology tools, and investigate whether cyber insurance would be an option for their business.

Best practices and recommendations

Small business owners

CFIB offers the following tips and best practices to make sure your business is protected against cyberfraud.

- **Be aware** of cyber risks to your business, using sources such as the Insurance Bureau of Canada, the Government of Canada's National Security and Defence Cyber Security Unit, CFIB's website and other business associations' websites and resources;
- **Raise awareness among employees** about cyberattacks and train staff to detect and avoid them;
- **Share information** on scams and best practices for prevention with other business owners in the community directly and through business associations;
- Evaluate whether **cyber insurance** would be advantageous for your business. The Insurance Bureau of Canada has information for business owners about cyber risks and cyber insurance; and,
- **Report cyberattacks** to law enforcement and other authorities, such as the Canadian Anti-Fraud Centre, the Competition Bureau, and the Better Business Bureau.

Governments, law enforcement and other authorities

CFIB makes the following recommendations to governments, law enforcement and other authorities (e.g. banks, insurance providers) to help prevent cyberfraud against small and mid-sized businesses in Canada:

- **Make sure resources are allocated adequately to "cyber policing"** and report yearly outcomes with specific numbers of interest for small businesses;
- **Help offset the costs of investing in IT protection equipment and programs** by providing small businesses with financial incentives (i.e., tax credit);
- **Proactively share information** on existing resources and best practices with businesses and associations; and,
- Provide **services specifically tailored to SMEs** on how to prevent cyberattacks and in regards to cyber insurance.

Appendix A

RESULTS: Your Business and Cyberattacks Survey

Survey method: Web
Survey period: October 15 – November 2, 2020
Tabulation date: November 2, 2020
Total responses 3,040
For comparison purposes, a probability sample with the same number of respondents would have a margin of 1 of plus or minus 1.8 per cent, 19 times out of 20.

% Response

1. Since March, have most of your employees been able to perform some or all their main responsibilities from a remote location (such as their home)? (Select one answer only)

- 12.6 Yes, the majority of my employees were able to perform *most* of their main responsibilities remotely
- 7.8 Yes, the majority of my employees were able to perform *some* of their main responsibilities remotely
- 79.6 No, the majority of my employees did not work remotely

2. Has your business' range of online activities (such as website orders with in-person pick up, online payments or reservations) changed since March? (Select as many as apply)

- 66.6 No change in my business' range of online activities *cannot be combined*
- 4.1 Yes, my business developed a website
- 9.8 Yes, my business started accepting online orders
- 3.4 Yes, my business started accepting online reservations
- 11.5 Yes, my business started accepting online payments
- 14.1 Other (Please specify)
- 1.6 Don't know *cannot be combined*

3. To what extent do you agree or disagree with the following statements? (Select one for each line)

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree	Don't know
Since March, I am more worried about potential *cyberattacks* on my business	18.3	38.0	19.2	13.5	11.0
I don't have the time, the knowledge or the resources to properly protect my business against cyberattacks	27.2	33.4	19.4	14.5	5.5

4. Which of the following applies to your business' experience with *cyberattcks* since March?
(Select as many as apply)

a. 4.9 My business has been a victim of cyberattacks (i.e. a cyber incident which resulted in the loss of money, goods, services, or valuable information)
b. 16.9 Cyberattacks were made against my business, but were unsuccessful (i.e. no loss in money, goods, services, or valuable information)
c. 74.9 To the best of my knowledge, my business has not experienced any cyberattacks *cannot be combined (Skip to Q8)*
d. 4.1 Don't know/Unsure *cannot be combined (Skip to Q8)*

If Q4 = b then ask Q5

5. Since March, which of the following types of cyberattacks were *used in an attempt* to defraud your business?
(Select as many as apply)

- 50.1 Malicious software (such as malware, spyware, Trojan)
- 83.0 Email scams and phishing (defined as an email designed to trick you into handing over personal/banking information or transfer money)
- 44.7 Supplier payments fraud (defined as a trick designated to make businesses wire money to a scammer's bank account thinking they are paying a supplier)
- 16.4 Other (Please specify)

If Q4 = a then ask Q6

6. Since March, which of the following types of attacks *resulted in the loss* of money, goods, services or valuable information for your business? (Select as many as apply)

- 53.4 Malicious software (e.g. malware, spyware, Trojan)
- 30.8 Email scams and phishing (defined as an email designed to trick you into handing over personal/banking information or transfer money)
- 21.8 Supplier payments fraud (defined as a trick designated to make businesses wire money to a scammer's bank account thinking they are paying a supplier)
- 29.3 Other (Please specify)

7. What impacts have cyberattacks had on you or your business since March? (Select as many as apply)

21.3	Loss of intellectual property (such as the business database) *cannot be combined*
30.1	Compromised personal/banking information
78.7	Loss of time to deal with the situation
26.5	Negative impact on business relationships (such as with clients, suppliers)
16.2	Hurt my business' reputation
24.3	Negative impact on *staff* morale
62.5	Negative impact on my *own* morale (stress)
50.7	Financial loss
14.0	Other (Please specify)

8. Other than your typical IT investments, has your business made any *additional* investments to protect your IT systems since March? (Select as many as apply)

67.5	No, my business did not make any additional investments in IT since March *cannot be combined* *(Skip to Q10)*
6.3	Yes, my business upgraded to *paid* software from *free* software
10.8	Yes, my business invested more in paid software
7.8	Yes, my business hired an external IT company
11.3	Yes, my business invested more in its own IT department or in external IT services we were already using
5.1	Yes, my business offered additional training to employees in matters of cybersecurity
4.3	Other (Please specify)
2.8	Don't know/Unsure *cannot be combined* *(Skip to Q10)*

9. Since March, how much has your business spent on additional investments to secure IT systems (such as antivirus software, training, external contractors)?
(Please enter approximate amount)

The results are calculated by excluding responses of less than $100 or more than $50,000.

Mean	**$6,700**

If Q4 = a or b then ask Q10

10. Please tell us more about your business experience with cyberattacks since March.

11. Does your business have *cyber insurance*?
(Select one answer only)

24.5	Yes, and I had it before March
1.7	Yes, I purchased a plan since March
13.2	No, but I'm considering it for the future
43.5	No
17.1	Don't know/Unsure

"Cyberattacks"
A cyberattack is any attempt to damage someone's computer system, steal the information on it or steal money from someone using the internet.

"Cyber insurance"
Cyber insurance protects businesses and individuals from Internet-based risks such as data breaches.