Protecting against cyber threats: A guide for your small business

Learn about the evolving cybersecurity landscape and get actionable strategies to protect your business, customers and people against cyber threats.

TELUS® Business

Contents

For hackers, businesses like yours are "where the money is" ... 3

A data breach costs a lot more than you think 4

Small and mid-sized businesses are at heightened risk 5

The many cybersecurity
challenges businesses face every day 6

Protecting your business from cyberattacks:
A few steps to get you started 8

Partnering with the right managed service provider 9

For hackers, businesses like yours are "where the money is"

When asked why he robbed banks, American criminal and FBI Most Wanted Fugitive Willie Sutton answered: "Because that's where the money is." The growing and always-evolving industry of cybercriminals might offer a similar answer if asked why they're increasingly targeting businesses like yours. After all, unless your organization is a large enterprise with thousands of employees and an extensive IT department, hackers have good reason to be confident that:

Your company may not invest heavily in protecting your digital infrastructure

53% of small Canadian business owners say they can't spare the costs to adopt new cybersecurity tools, even to protect sensitive customer data.[1]

Your employees could be easy targets for phishing or other social engineering scams

34% of small and midsize Canadian businesses provide mandatory employee training on basic cybersecurity awareness.[2]

Your team may not be able to mitigate the risk of a hacker infiltrating your network

16% of small businesses across Canada feel confident they'd know what steps to take in the event of a cyberattack.[3]

Safeguarding your business against cyber attacks

A recent Mastercard study shows small Canadian business owners need additional support to effectively prevent and recover from cyberattacks.[4] With that in mind, this guide highlights the importance of prioritizing cybersecurity as a must for businesses. You'll learn about some of the sophisticated tactics used by cybercriminals, and the types of best practices and solutions that can help protect your company from attacks and data breaches.

What is a data breach?

The Government of Canada describes this type of cybersecurity threat as **"an act or event that results in the compromise of sensitive information or assets."**[5] This means that there has been unauthorized access, disclosure, destruction, removal, modification, use or interruption of protected and classified information and assets.

A data breach costs a lot more than you think

Before exploring strategies for fortifying your company's cybersecurity, it's worth assessing the risk and the true cost of a data breach. The TELUS Canadian Cloud Security Study found that businesses across the country are hit with an average of five cyberattacks per year, carrying direct costs of approximately CAD $88,000 for each incident.[6]

A Canadian Federation of Independent Business (CFIB) study found that nearly half (45%) of Canadian small businesses were hit with a cyberattack in the previous 12 months.[7] This data suggests that there's nearly a 50-50 chance that your business will suffer at least one cybersecurity incident in the coming year.

In addition to the direct costs, the study also found many indirect costs affecting these businesses. These costs are not as easy to quantify but can cause damage to the business over the long-term.

Businesses across Canada are hit with an average of five cyberattacks per year

$88,000/ incident.

For example, after a serious cyberattack, the victimized business is likely to experience:

- Decreased employee productivity
- Lost trust from customers
- Negative media coverage
- Weakened relationships with partners
- Damaged reputation with the public

Small and mid-size businesses are at heightened risk

A 2023 Insurance Bureau of Canada (IBC) survey found that most small and mid-size businesses assume their size will help them fly under cybercriminals' radar.[8] Attacks against them don't receive the same headlines, but Canadian small and mid-size businesses are regularly victims of cybercrime.

Your business isn't small enough to fly under hackers' radar

45% of small businesses in Canada experienced a random cyberattack in the previous year.[9]

60% of Canadian small businesses believe they're "too small" to be the target of cybercriminals.[10]

27% of small businesses have suffered a targeted attack within the previous year.[11]

Cybercriminals can find it easier to hack smaller companies

Hackers and their organizations are becoming more sophisticated over time. They methodically study the pool of potential victims and seek out the ones they believe offer the highest chances of a payoff.

Cybercriminals will continue to evolve their tactics, according to the Government of Canada[12], including targeting more small and mid-sized companies, in order to avoid attention-grabbing, higher-profile attacks. Cybercriminals also know that smaller companies are more resource-constrained and often need to prioritize other operational expenses over IT and cybersecurity. Those realities, the hackers assume, make these businesses easier targets than large enterprises.

Unfortunately, hackers are often correct in this assumption. As the CFIB study also found, despite the high rates of attacks against them, only 11% of business leaders running small and mid-size organizations offer mandatory cybersecurity training to their employees.[13]

Even taking the more encouraging statistic from the Insurance Bureau of Canada (IBC) that 34% of employees say they receive mandatory cybersecurity training[14], that number should still be cause for concern, because it means two-thirds of employers don't teach their staff basic safety measures for protecting their companies' data and digital infrastructure.

The decision to prioritize other areas of the business represents a significant missed opportunity. Cybersecurity training for all employees could help reduce what our own TELUS Canadian Cloud Security Survey found to be the top cause of cyberattacks – human error.[15]

As the IBC survey found, 69% of small business owners don't even consider fortifying their digital environments a financial priority.[16] Cybersecurity is essential to your company's bottom line, your ability to continue operating and even your reputation and trust with customers and the public.

Cybersecurity risks are becoming more prevalent and widespread than ever, making this the best time to explore ways to strengthen your business' security.

69% of small business owners don't even consider fortifying their digital environment as a financial priority.[16]

The many cybersecurity challenges businesses face every day

Much of today's discussion about cybersecurity focuses on the fact that hackers are always evolving, updating their tactics, searching for new vulnerabilities, learning from past mistakes and becoming more sophisticated. This is true and definitely important to keep in mind.

Another key challenge you're likely facing is simply that in today's connected world, your business has had to significantly expand their digital footprint. You're adopting new software tools, moving more data to the cloud and allowing your staff to access company content outside your offices and even on their own personal devices.

These new digital workflows, combined with the fact that your employees aren't learning how to protect your data, are opening new doors for those ever-evolving hackers. Below are just a few examples of the dangers your business may be facing.

You're storing, accessing, and sharing more sensitive company data across a growing number of cloud platforms

The TELUS Canadian Cloud Security Study found that businesses today are using an average of 8.5 different large-scale cloud platforms: Amazon Web Services, Microsoft Azure, Google App Engine, Microsoft 365, Dropbox, Slack, etc.[17]

The average varies according to the size of the business. Large enterprises (1,000+ employees) use 8.1 different cloud platforms, while smaller businesses (under 250 employees) average 11.8 solutions.

If your teams are using the cloud-based services listed above do you readily know whenever one of these vendors sends its customers a security warning? Do you always know as soon as these vendors issue patch recommendations or suggestions to move to an updated version due to a security vulnerability?

If your company doesn't have a systematic process to receive and act on warnings for every app, operating system, network and tool across your digital environment, you could be leaving your IT infrastructure open to cyberattacks. After all, you can be sure that the hackers themselves are monitoring those vendors' security warnings.

Your employees are accessing company systems, apps, and data on unsecured networks

Since the pandemic, you likely have more employees than ever working either remotely or under a hybrid arrangement. That means more of your staff doing their work – and accessing sensitive corporate data – at coffee shops, restaurants and other public places over unsecured Wi-Fi and cellular networks.

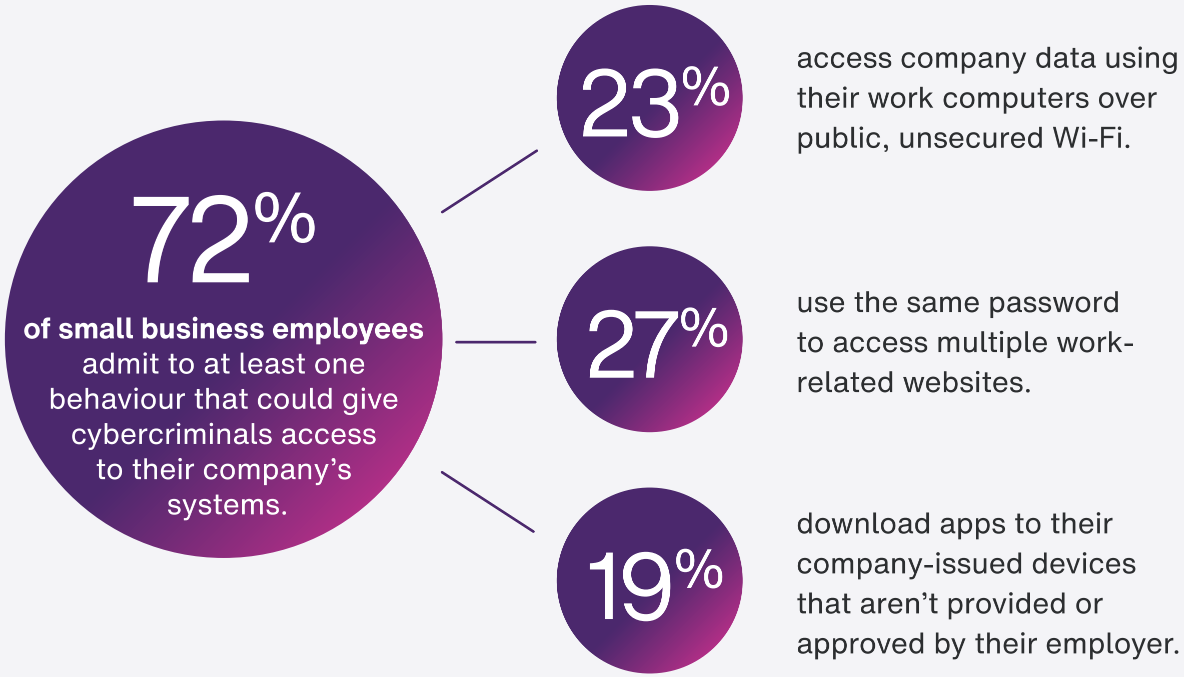
Cybercriminals are also aware of this. They know the rise of remote work in the last few years means more sensitive, lucrative data than ever – including company logins and passwords – now traverses the internet outside the protections of the corporate firewall.

That helps explain why, as the Mastercard Research report found, cybercrime in Canada has increased by more than 600% since the start of the COVID lockdowns.[18]

Your employees might be vulnerable to the most basic tricks in the hackers' book

If you're among the majority of businesses that don't put employees through mandatory training on how to safely handle company data and digital systems, you could be facing an ongoing security vulnerability that all the high-cost cybersecurity tools can't solve. As a 2023 study reported in Security Today found, 88% of data breaches against businesses are caused by employee mistakes – making it by far the leading cause.[19]

To get an idea of how these common mistakes can expose your company to a successful hack, consider these admissions from the employees surveyed in 2022 by the Insurance Bureau of Canada:[20]



72%

of small business employees admit to at least one behaviour that could give cybercriminals access to their company's systems.

23% access company data using their work computers over public, unsecured Wi-Fi.

27% use the same password to access multiple work-related websites.

19% download apps to their company-issued devices that aren't provided or approved by their employer.

Even if you've given your employees some basic cybersecurity awareness training – telling them, for example, not to open email attachments from unknown senders – you're far from done. Keep in mind, cybercriminals' tactics are always getting more advanced.

That means you'll need to build a company culture where using cybersecurity best practices is a part of your employees' day-to-day jobs – not a one-time topic only thought about during training. You'll want to bring your teams together for regular refresher lessons, simulations to test their readiness and introductions to new known attack strategies as soon as you learn about them.

The 2022 Canadian Federation of Independent Business survey, for example, found that 11% of small companies had fallen victim in the previous year to a specific type of phishing called "whaling," where the hacker pretends to be the company's CEO or another senior leader.[21]

Those employees might have become skilled at spotting the standard types of phishing emails. But then hackers realized they could add a new sense of urgency – and undermine their target's normal skepticism – by pretending to be a top executive at the employee's company.

Protecting your business from cyberattacks: A few steps to get you started

There is no set of technologies, tools or processes you can roll out that will guarantee your business avoids a data breach, but you can make it far more difficult for cybercriminals to attack. We've put together a comprehensive list below to help you develop a defence-in-depth (DiD) strategy. The following list of entry-level cybersecurity measures is far from complete, but it represents a strong starting point from which your team can continually build a more comprehensive security environment – and begin building cybersecurity into your company culture.

Implement password-management guidelines and tools for your employees

A 2023 Better Business Bureau report found that the top-used passwords by Canadian employees included "Canada," "hockey" and "123456".[22]

Train your employees on how to create more complex passwords while stressing the risk of using simple or repeated passwords. Better yet, if you have the budget, find a password-management application that can create and monitor your staff's passwords. Multi-Factor Authentication (MFA) can also help add an extra layer of security beyond a username and password.

Implement a patch-management strategy

According to the TELUS Cloud Security Study, chances are your employees are using between 8 and 12 different large-scale cloud services, such as Google or Amazon Web Services, as well as many other workflow applications.

Take inventory of all the tools and digital environments where your staff creates, stores and accesses your proprietary data. Then you will need to create a process – or assign responsibility to one or more employees – to monitor these vendors' notices about new patches, necessary system updates or security warnings.

Implement a secure data-backup and recovery solution

Backing up your data to a secure, offsite environment is an important step to take for several reasons, including the ability to quickly resume business operations if your primary systems fail or your area suffers a natural disaster. But keeping your data backed up and separate from your main corporate network can also help make you less vulnerable to a ransomware attack. If you can access your mission-critical company information even after the hacker encrypts and locks you out of your primary network, that cybercriminal can't stop critical business from running.

Train your employees on cybersecurity and update their training often

As effective as the right cybersecurity solutions can be if implemented and managed properly, their effectiveness can be undercut if your employees unwittingly hand the digital keys over to a clever hacker.

Here are some important topics to cover when rolling out cybersecurity training for your employees:

- The most common phishing and other social engineering tactics.
- The dangers of opening files or clicking attachments from senders they don't know.
- Security awareness to help employees detect and distrust unknown networks so they can avoid and report them.
- How to connect securely through a Virtual Private Network (VPN).
- The need to create complex, difficult-to-guess passwords for all work-related apps, systems and devices.

Cybersecurity training can help to raise employee awareness of the importance of cybersecurity, which can lead to better security practices overall. Given the increasing sophistication of cyberattacks, it is clear that cybersecurity training is not a luxury for small businesses. It is a necessity. By investing in cybersecurity training, small businesses can help to protect themselves from the most common cyberattacks and keep their data safe.

Partnering with the right managed service provider

If your company is adding "IT responsibilities" to the job descriptions of employees in other departments, or if your internal IT team is overwhelmed with multiple priorities, the chances are high you're not fully addressing your ongoing data-security threats. No matter how much time and effort those committed employees spend trying to keep up with these issues, they don't have the experience or background to see the full – and always-changing – picture of cybersecurity.

Outsourcing your cybersecurity can help protect against threats – from customization to implementation, management and proactive monitoring. The right partner can help develop a Defence-in-Depth (DiD) strategy, so you can prioritize what solutions to invest in and actions to take over time to protect your business.

TELUS Business takes a comprehensive approach to your cybersecurity, including both a best-in-class technology stack and proactive monitoring to keep your business and employees safe. Our Virtual Chief Information Officer (vCIO) can create tailored roadmaps to help implement and administer a best-practice environment to to better protect your digital infrastructure. You get the most advanced cybersecurity tools and technologies, combined with dedicated IT professionals to deploy a multi-layered security strategy to help safeguard your organization from cybercriminals.

Connect with a managed IT specialist today to learn how we can help with your evolving IT needs.

Visit telus.com/**FullyManaged**

Take IT issues off your to-do list with TELUS Fully Managed

Our managed IT services provide comprehensive support for a wide variety of day-to-day IT needs including **managing user accounts, updating workstations, and maintaining servers, networks and Microsoft 365 services.**

Cybersecurity services

We offer a multi-layered approach to security to protect against cyber threats and data loss with the latest security tools, proactive monitoring and secure backups.

24/7 helpdesk

We assist users with IT issues and requests to reduce time spent troubleshooting. Our deep pool of experts can support 24/7 IT uptime and business continuity.

Cloud migration

We help assess, plan and modernize services in the cloud for impactful cost savings, enhanced capabilities, improved security and the ability to work from anywhere.

Tech strategy

Our Virtual CIO (vCIO) team works with customers to develop business-aligned IT strategies that help drive impact and get a higher return on IT investment.

Continue learning

Blog

Protecting your business against hidden threats

Read more

Blog

5 Ways businesses can benefit from managed IT services

Read more

Blog

5 Tips for choosing the perfect managed IT service provider

Read more

References

1. Mastercard Research: Canadian small business owners need support to prevent cyberattacks (2023)
2. IBC: Only 34% of small and midsized business employees receive cyber awareness training (2022)
3. Mastercard Research: Canadian small business owners need additional support to effectively prevent cyberattacks (2023)
4. Mastercard Research: Canadian small business owners need support to prevent cyberattacks (2023)
5. GoC: Reporting security incidents and changes in circumstances and behaviours (2023)
6. TELUS: The TELUS Canadian Cloud Security Survey (2022)
7. CFIB: CFIB launches new education program to help business owners improve their cybersecurity (2022)
8. IBC: Small businesses are underestimating their cyber risk (2023)
9. CFIB: Half of small businesses falling prey to cyberattack (2022)
10. GoC: Reporting security incidents and changes in circumstances and behaviours (2023)
11. CFIB: Half of small businesses falling prey to cyberattack (2022)
12. GoC: Reporting security incidents and changes in circumstances and behaviours (2023)
13. IBC: Only 34% of small and midsized business employees receive cyber awareness training (2022)
14. CFIB: Half of small businesses falling prey to cyberattack (2022)
15. TELUS: The TELUS Canadian Cloud Security Survey (2022)
16. IBC: Only 34% of small and midsized business employees receive cyber awareness training (2022)
17. TELUS: The TELUS Canadian Cloud Security Survey (2022)
18. Mastercard Research: Canadian small business owners need support to prevent cyberattacks (2023)
19. Security Today: Why are so many cyber breaches due to human error (2023)
20. IBC: Results of a survey of 1,525 Canadians that work at small and medium-sized businesses (2022)
21. CFIB: Half of small businesses falling prey to cyberattack (2022)
22. Better Business Bureau: Risky password management continues to be a problem (2022)