Cybersecurity assessment report

Developed by Mastercard

EXPAND VERSION

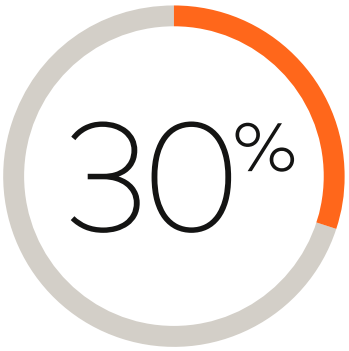
Contents

This cybersecurity assessment report is meant for educational purposes only. Though your score may improve; it is not an indication of cybersecurity protection for your business.

Introduction

In an era where businesses thrive on digital innovation and connectivity, the importance of robust cybersecurity cannot be overstated.

Your cybersecurity score



Small businesses, often considered the lifeline of our economy, are not immune to the evolving landscape of cyberthreats. As your trusted ally, Mastercard developed a cybersecurity assessment process to help you evaluate the knowledge of your current cybersecurity practices.

Based on your responses to the cybersecurity assessment, we generated this report to provide you with an overview of your current knowledge with cybersecurity posture. The report also offers strategic recommendations to help you fortify your defences against cyberthreats.

Expand your knowledge

As a key decision-maker within your company, you have many tasks — including ensuring that confidential business and customer data is protected. You've put security processes into place, but unseen vulnerabilities can still put your organization at risk. Many top risks are due to internal human behaviour and compromised or stolen devices. Let's get started on further enhancing your security knowledge!

Cybersecurity: Importance, stakes and impact

You have worked hard to design, launch and grow your business. Your employees depend on your business for their livelihoods. Your customers trust your business to provide high quality goods and services, timely delivery and excellent customer service. Customers also count on your business to keep their personal data and credit/debit card information secure.

Sadly, many small business owners don't take the time to secure their business's digital ecosystem. Cybercriminals know small businesses can be an easy target.

"Nearly 50% of all cyberattacks are against small and medium businesses, putting them at risk of great financial loss that may even lead to business closure."

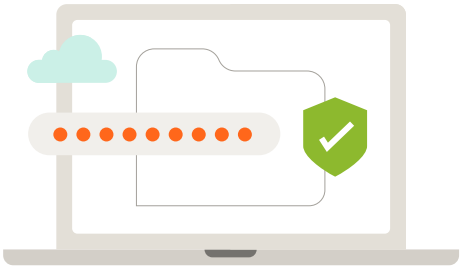
Your business can be impacted in the following ways in case of a cybersecurity breach scenario:

- **Business interruption:** A cyberattack may disrupt normal business operations, making it difficult for businesses to operate smoothly. This can mean obstructed access to your billing system and your customer contacts or a halted production line. A cyberattack may also lead to the closure of businesses permanently, if the financial or reputational damage is severe.
- **Loss of sensitive data:** Refers to the situation where confidential or valuable information, such as financial data, trade secrets and customer information, is accessed, copied or deleted by an unauthorized individual. This information is valuable for businesses as it often lays the foundation of their operations.
- **Financial losses:** Refers to monetary losses a business incurs due to a cyberattack, which may also result in loss of revenue. Moreover, companies may be required to pay legal fees, ransom or other costs associated with managing a cybersecurity breach.
- **Reputational damage:** A data security breach causes reputational damage that can impact current and future sales. Eighty-seven percent of consumers say they will take their business elsewhere if they don't trust a company is handling their data responsibly.
- **Legal consequences:** Businesses may be subject to fines, lawsuits and regulatory actions for failing to protect the data.

Business owners and employees who learn and follow cybersecurity best practices can reduce the risk and the fallout of a cyberattack. Fortunately, there are simple steps you and your employees can take to improve cybersecurity and help your business thrive. Read this report to learn more about cybersecurity best practices and how you can implement them within your own digital environment.

Cybersecurity solutions: An expense or an investment?

Embedding cybersecurity as part of your business strategy means making sure your company is well-protected against online threats and attacks.



It involves taking proactive steps to safeguard information, customer data and the overall integrity of your systems.

Installing cybersecurity measures in an organization requires some initial investment that companies are hesitant to make, and so they choose to operate unshielded.

Let's look at an example of cost-benefit analysis to understand this concept:

You were supposed to invest $19,000 (the average amount a small business spends on cybercrime prevention and detection in Canada) on cybersecurity. Seeing the amount, your organization decided not to invest now. A few months down the line, your company was held at ransom by cybercriminals demanding $200,000 to free the servers, machines and data. Now, you don't have any option but to pay the ransom. The initial investment of $19,000 could've helped you secure the organization against such security threats and save $200,000. A long-term investment, cybersecurity solutions can help you build reputation and foster customer trust.

Cybersecurity awareness and training

Employee training initiatives should include continuous education on cybersecurity policies and best practices for both new and existing employees.

Below are the benefits of cybersecurity training for employees:

- Your business's cybersecurity is only as strong as your weakest link. This is why cybersecurity training for employees is a crucial element to protect your business.
- Cybersecurity training helps secure your business from cyber risks by making employees aware of the potential threats and traps.

Elements to include in your cybersecurity training:

- Strong, unique password usage and two-factor authentication
- Operating system, software and application updates/patching for personal devices and business accounts
- Phishing recognition and response
- Safe USB use
- Data backup and recovery
- Cyberattack response and recovery plan for the business

Access management: Limiting access rights

Grant employees access to business devices, operating systems, software/applications and online accounts only when it's necessary to perform their duties.

Evaluate every employee's business needs to access devices, operating systems, software/applications and online accounts. Don't grant logon access and permissions to those who don't need to use these digital assets. You can limit your business's exposure to cybersecurity risks by limiting the number of employees with access rights.

To learn more about access management best practices from Mastercard, watch this helpful video.

Scan and protect with antivirus software

A computer virus is a type of malicious software or malware that spreads among devices and damages the data and software.

Cybercriminals use software viruses to disrupt systems and cause major operational issues, and the result is data loss and leakage.

Install antivirus software that scans and removes viruses in real time before they can cause damage. Failing to install antivirus software on all your devices leaves them susceptible to computer viruses that can disrupt your business.

To learn more about antivirus software and best practices from Mastercard, watch this helpful video here.

Be mindful of phishing attacks

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

It occurs when an attacker poses as a trusted entity and dupes the victim into opening an email, instant message or text message.

Phishing attacks can have devastating results, including unauthorized purchases, theft of funds or identity theft. Phishing is also used to gain a foothold in corporate or government networks as a part of a larger attack. For organizations, phishing attacks may cause financial losses, in addition to loss of market share, reputation and consumer trust.

Phishing attacks can be of the following types:

- **Email phishing:** This is the most common form of phishing in which attackers send out fraudulent emails that can net significant information and money. Attackers design phishing emails to mimic actual emails from trusted organizations by copying their phrasing, typefaces, logos and signatures to make the messages appear legitimate.
- **Spear phishing:** Spear phishing targets a specific person or enterprise as opposed to a random person or team. Such targeted phishing attacks require special knowledge about the organization, including its power structure.
- **Smishing:** This is a form of social engineering attack that relies on exploiting human trust rather than technical exploits. Cyberattackers use simple text messages instead of emails to send you either malware or links to malicious websites.
- **Vishing:** Vishing is phone call phishing. Avoid answering phone calls from unknown phone numbers to safeguard from vishing attacks. Instead, listen to phone messages from unknown callers and follow up by calling the customer service phone number posted on the organization's official website.

Below are some best practices to avoid phishing scams:

- Don't open emails from senders you don't know.
- Check the sender's email address or any other identifying information (for example, company logo, address and contact details) for inconsistencies, misspellings or signs it may be fake.
- Don't click on links or download attachments in an email if you are unsure of the legitimacy of the sender.
- Don't provide account or personal information.
- Delete suspicious emails and then empty the trash folder.
- Inform your employees about suspicious emails and ask them to not click on them.
- Don't respond to text messages from unknown senders or seemingly legitimate senders that ask you to provide personal or account information. Instead, follow up by calling the customer service phone number posted on the organization's website.
- Cultivate a culture of sharing information about phishing attempts to familiarize your team with latest tactics and include these new trends in security trainings and onboarding of new employees.

Cover blind spots with software patching

Software patching provides important updates from developers and software providers.

The old phrase "Patch Tuesday leads to exploit Wednesday" is commonly used by hackers to exploit vulnerabilities that are still not patched post patch release. This is quite often the case for cybersecurity breaches, especially for smaller organizations that do not stay on top of their patch management schedule.

All your business's digital assets (software, operating systems and applications) across computers, phones, printers, routers and more can be used as a weapon against your business if they are not updated (patched) regularly and on time.

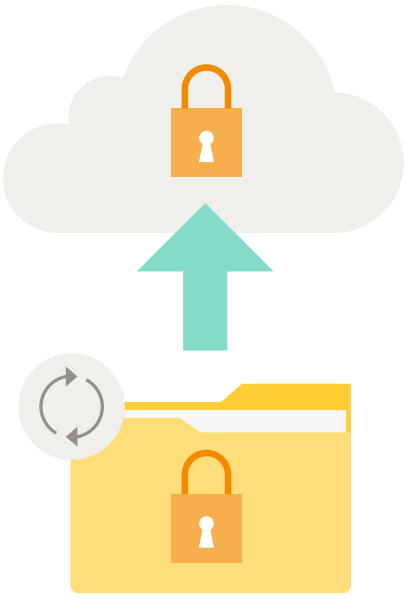
Below are the steps you can take to make sure software, operating systems and applications are always up to date:

- Set up automated updates to ensure that updates are launched as soon as they are available. Take stock of what software you currently use across phones, printers and other devices and make sure it is always up to date.
- Promptly update or patch known security and programming issues to reduce the likelihood of cybercriminals exploiting your digital assets.

To learn more about software updates best practices from Mastercard, watch this helpful video.

Back up today for a safer tomorrow

Securely backing up and storing your critical data allows you to keep your business up and running even after a data breach or ransomware attack.



Here are a few more reasons to back up your data regularly:

- Computers can fail without warning. If data is not backed up, you risk losing everything. This loss of data can include anything from customer contact information to your invoice and billing system.
- Accidental deletion of files is a common issue, which makes it is important to regularly back up data, especially important files.
- Losing mission-critical information can lead to loss of productivity, financial losses and stalled projects.

Below are the best practices for data backup and recovery:

- Identify your company's critical data
  - Implement personal identifying information (PII) for customers and employees to protect the company's critical data. Examples of PII include full name, maiden name, mother's maiden name or alias. PII also includes personal identification numbers, such as social security number (SSN), passport number, driver's licence number, taxpayer identification number, financial account numbers and credit card numbers.
  - Additional critical data includes supplier information and business data such as sales data, intellectual property, financial data and other data crucial for your business operations.
- Securely back up your business systems
  - Securely backing up and storing your critical data allows you to keep your business running after a data breach or ransomware attack. Attackers can either completely wipe out the data or hold it for ransom.
  - Secure online backup options include cloud storage and online backup services. Alternatively, you can back up your data on an external hard drive stored in a locked fireproof and waterproof location. However, this option is less secure and convenient.
  - Reduce the risk of an administration account being compromised by setting up multi-factor authentication (MFA) for all backup activities.

To learn more about data backup best practices from Mastercard, visit resources available here.

Managing data breaches

Digital security is particularly top of mind for small business segment in Canada as two-thirds of small business owners have experienced at least one security threat, with phishing and malware being the most common. A recent study from Palo Alto Networks Canada found that **the average ransom paid by Canadian businesses has increased by nearly 150% in two years, amounting to more than CA$1.13 million. Additionally, the average ransom demanded steeply rose by 102%, from CA$449,868 in 2021 to CA$906,115 in 2023.**

A cyberattack or a data breach could be a very distressing situation for you and your team. Identify what you need to protect (personal information, IP and more) and develop a cybersecurity action plan and a cyberincident response plan. You can better appreciate the importance of your business's online security by understanding the consequences of failing to protect your digital assets or losing access to information. Having a clear line of sight will help you to develop a plan on how best to respond, limit and eradicate security threats or the damages caused to your business.

There are some predefined actions that you can take to address a specific security incident. This can include a bad actor getting access to your information or preventing you from accessing it, malware infection, violation of security policies, account takeover and more. The main goal here is to enable you and your team to respond to cyberattacks timely and effectively.

Follow the below steps to respond to a cyberattack:

1. Identify the affected systems, servers and networks to gauge the attack severity and plan a response accordingly.
2. Separate the affected machine from the main network to prevent other devices from getting compromised.
3. Delete infected or malicious files, prevent their execution, isolate affected device(s) from main network, disable accounts and scan disks with the help of the latest security software to limit further damage.
4. Notify all stakeholders of the incident in a timely manner so the appropriate steps can be taken to contain the damage. This includes the local police, financial institutions and credit bureaus (if financial data is compromised), Privacy Commissioner of Canada (if PII information is breached) and Canadian Centre for Cyber Security, reachable at 1-833-CYBER-88 or 1-833-292-3788.
5. Clean up all traces of the attack by deleting infected/malicious files, and schedule critical tasks and services to help your business recover. In case you are not able to perform these operations on your own, seek professional help from cybersecurity companies who specialize in handling cyberattack and restoration process.
6. Restore systems from backup data to resume business as usual.

Building resilience against cyberthreats

Cybersecurity is not a one-time effort but an ongoing commitment to protect your business and its stakeholders.

This assessment report aims to serve as a roadmap for your organization to navigate the ever-evolving threat landscape with confidence and resilience. This report is meant for educational purposes.

We appreciate your commitment to the security of your business. If you are interested in learning more and partnering with Mastercard, please reach out to a Mastercard representative.