Cybersecurity assessment report

Developed by Mastercard

EXPERT VERSION

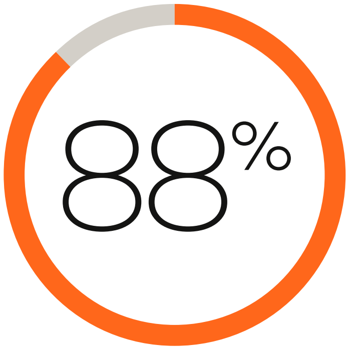
Contents

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 has developed a cybersecurity assessment process to help you evaluate the knowledge of your current cybersecurity practices in your business.

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

Master your security

It's been your mission to create a secure cyber environment for your company. Although you've implemented many effective security protocols, fraudsters' tactics and strategies are constantly evolving — putting your data and the trust of your customers, lenders and employees at risk. You can stay ahead of the bad actors by consistently updating your security tools and protocols. Let's get started to further enhance your security expertise.

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 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 can even lead to business closure."

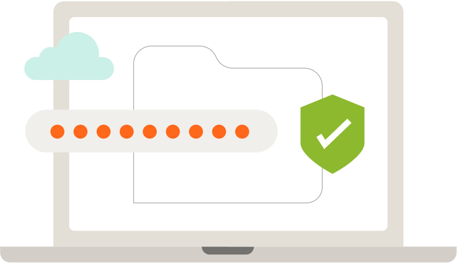
Your business can be impacted the following ways in case of a cybersecurity breach scenario:

- **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 to the businesses as it often lays the foundation of operations.
- **Financial losses:** Refers to monetary losses that a business incurs due to a cyberattack, which may result in loss of revenue. Moreover, companies may be required to pay legal fees, ransom or other costs associated with managing and remediating 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 fallout of a cyberattack. Fortunately, there are easy 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 that 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 a 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 later, your company was held at ransom by cybercriminals demanding $200,000 to free the servers, devices 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 your organization build its reputation and foster customer trust.

Crown jewels analysis

Crown jewels are the assets, applications and systems that are mission critical to your business and are a high value target for cybercriminals.

It's important to identify these assets and define additional security measures around them for higher security. For starters, maintain an up-to-date list of your devices, operating system, software, applications and online accounts to understand the risks and better protect your business. The list will also help keep track of system updates and defend against cyberattacks.

Store, protect and share with password managers

It is a tool that provides users and businesses with the ability to track, store, protect, share and manage login credentials for applications and online services. It is crucial to keep users safe and secure online.

Password managers store passwords in secure, cloud-based digital vaults. This allows users to access their login information anywhere, using any device. The master password is the only one that users must remember.

The following are reasons why you should use a password manager:

- No need to memorize multiple passwords
- Increased protection against phishing
- Share sensitive information securely
- Auto-generate highly secure passwords

Enhance security for Internet of Things

Internet of Things (IoT) refers to a network of physical devices connected via sensors, processing ability, software and other technologies.

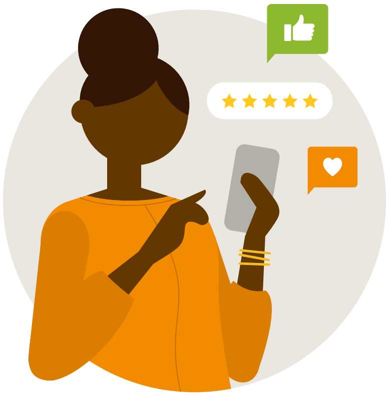
These devices can exchange data with other devices and systems over the internet or other communications networks. Listed below are a few threats associated with IoT devices:

- Device exploitation
- Insecure networks
- Data breaches
- Lack of security updates

To ensure security for IoT devices, each IoT device should have a unique, complex password to help protect against a cyberattack that could result in service disruption, data theft, data or service manipulation and/or noncompliance with government standards.

To learn more about Internet of Things (IoT) best practices, visit resources available here.

Maintain social media security



Cybercriminals can use information about you and your employees posted on social media to launch several types of cyberattacks, including phishing attacks, malware and ransomware attacks, disinformation campaigns, identity theft and more.

Be very careful about what personal information you share on social media sites. Sharing too much information might help cybercriminals piece together aspects of your life that open the doors to various types of cyberattacks.

To learn more about social media security best practices, visit resources available here.

Pump up mail security with enhanced email filtering

Enhanced email filtering is a tool that inspects all emails before they are delivered to your inbox.

This tool helps protect against phishing attacks by detecting and blocking emails that contain attachments and links known to be harmful. Enhanced email filtering tools provide more protection than typical spam filters and can be adjusted to fit your preferences.

To learn more about enhanced email filtering best practices from Mastercard, visit resources available here.

Prepare a ransomware response plan

Ransomware is a type of malware (bad software) that blocks access to a system, device or file until a ransom is paid or you get access to a decryption key that can unlock your data.

Developing a documented response plan will place you in a much better position to deal with a ransomware attack.

Your ransomware attack response plan should include the following:

- Risk assessment metrics that provide details about affected data/systems/servers to help you estimate the severity of an attack
- Scheduled, automated data backups
- Security policies and procedures
- Cyberincident response team
- Key internal and external stakeholders
- Communication guidelines, including notification details to affected individuals and stakeholders

To learn more about ransomware response plans from Mastercard, visit resources available here.

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 implementing cybersecurity training for employees:

- Your business's cybersecurity is only as strong as your weakest link. This makes employee cybersecurity training 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, including on personal devices and accounts used for business
- Phishing recognition and response
- Safe USB use
- Data backup and recovery
- Your business's cyberattack response and recovery plan

To learn more about cybersecurity awareness and training from Mastercard, visit resources available here.

Scan and protect with antivirus software

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

Cybercriminals use software viruses to disrupt systems and cause major operational issues that can result in 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.

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 cyberthreat, 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 almost 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. Knowing what you are protecting (personal information, IP, etc.) and understanding the consequences of failing to do so are particularly important when you think about your business's online security. Having a clear line of sight will help you to develop a plan on how best to respond, limit and eradicate the security threat and damage caused to your business.

There are some predefined actions that you can take to address a specific cybersecurity incident. This can include scenarios of 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 quickly and effectively to minimize the potential damage caused by the attack.

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/malicious files, prevent their execution, isolate affected device(s) from the 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 are taken to contain the damage. This includes the local police, financial institutions and credit bureaus (if financial data has been compromised in the breach), Privacy Commissioner of Canada (if PII information is breached) and Canadian Centre for Cyber Security, reachable at 1-833-CYBER-88 and 1-833-292-3788.
5. Clean up all traces of the attack by deleting infected/malicious files and create scheduled tasks and services. 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

Cyberthreats are ever present and evolving. 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. The 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.