Cybersecurity assessment report

Developed by Mastercard

BASIC VERSION FOR UNITED STATES SMALL AND MEDIUM BUSINESSES (SMBs)

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 in your business.

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

Learn the basics

Many budding entrepreneurs or owners of smaller businesses can feel anxious just thinking about implementing cybersecurity solutions. But protecting your and your customers' data is crucial — and less difficult than you may think. Let's get started!

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.

39% of U.S. small and medium businesses surveyed experienced a cyberattack that resulted in 29% losing customer trust, 29% experiencing revenue loss and 12% closing their business[1]

Source:

1. 2025 Mastercard Proprietary Research: SME Cybersecurity Landscape – U.S. Report

2. 35 Alarming Small Business Cybersecurity Statistics for 2025 | StrongDM

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 permanent closure of businesses if the financial or reputational damage is severe.

- **Loss of sensitive data:** This is a 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 businesses, as it often lays the foundation of operations.

- **Financial losses:** This refers to monetary losses that 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 and remediating a security breach.

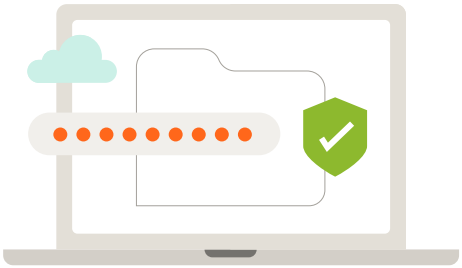
- **Reputational damage:** A data security breach causes reputational damage that can impact current and future sales. Fifty-five percent of U.S. residents report being less likely to continue doing business with firms that are breached.[2]

- **Legal consequences:** Twenty-four percent of U.S. businesses that experience a cyberattack are subject to lawsuits due to data breach and other customer impacts, and 15% file for bankruptcy.[1]

Business owners and employees who learn and follow cybersecurity best practices can reduce the risk and the 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 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. Proactively investing in cybersecurity can save money in the long run. Eighty-seven percent of SMBs in the U.S. that have experienced a cyberattack now work with a cybersecurity solution provider, and 88% report they are more focused on prioritizing cybersecurity investment.[1]

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 the cost-benefit analysis to understand this concept:

Imagine your business is considering a cybersecurity investment of $21,000 — the average amount small businesses in the U.S. spend on cybersecurity prevention, detection and setup. However, seeing the cost, your business decides to delay the investment.[2]

A few months later, your business is hit by a ransomware attack. Cybercriminals demand $46,000 - the median ransom demand, but more than 50% of SMB victims paid more than $100,000 — to unlock your servers, machines and data. With operations at a standstill, you may have no choice but to pay the ransom just to get back up and running.[3]

Had you invested the $21,000 earlier, you could have avoided the attack and saved your business from $25,000 to $79,000 in losses and downtime. Cybersecurity is not just a cost, it's a long-term investment that protects your operations, builds your reputation and fosters customer trust.

Source:

1. 2025 Mastercard Proprietary Research: SME Cybersecurity Landscape – U.S. Report

2. 35 Alarming Small Business Cybersecurity Statistics for 2025 | StrongDM

3. 2025 Cyber Attack Report: Data Breaches Are Costing Small Businesses | SmartFinancial

Implement strong password guidelines

Passwords are the first line of defense against cyberthreats, and therefore, you should follow password standards to make sure your data, devices, networks and servers are safe.

Mentioned below are some best practices to maintain password security:

- Strong passwords should be 14 to 20 characters long and include upper- and lowercase letters, numbers and characters.
- Never reuse the same password on multiple accounts.
- Never share your passwords with others.
- Use a trusted password manager application.
- Change your password if your account is compromised.
- Use two-factor authentication wherever available.

To learn more about password best practices from Mastercard, watch this helpful video from Mastercard to learn more: Use Strong Unique Passwords

As your business grows, the number of devices, systems, applications and servers also grow, requiring you to remember different passwords for different accounts. To keep things simple, efficient and secure, we recommend businesses use a **password manager** — a tool that provides users and businesses with an ability to track, store, protect, share and manage login credentials for applications and online services.

Password managers store passwords in secure, cloud-based digital vaults. This allows users to access their login information from 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:[1]

- Your passwords are too simple.
- Password managers include random password generation.
- You only need to remember one password.
- The numbers are against you as your number of passwords grow.
- Passwords will always be at the ready with device syncing.

Source:

1. 5 Reasons Why You Should Use a Password Manager

Enhance security with two- and multi-factor authentication

Two-factor (2FA) and multi-factor (MFA) authentication is an extra layer of protection used to ensure the security of online accounts beyond just a username and password.

Watch this helpful video from Mastercard to learn more: Implement Multi-Factor Authentication (MFA)

2FA/MFA options include a text message or an email sent to your mobile phone or computer with a one-time code. Another 2FA/MFA method is biometric authentication, such as thumbprint or facial recognition on your mobile phone.

There are three methods to enable 2FA to step up authentication:

- **2FA hardware tokens:** Hardware tokens for 2FA are usually available as USB devices that generate one-time passwords at the time of log in. To perform 2FA using a hardware token, simply insert the USB device into the USB port of your machine. Enter your password and click on the hardware token field for second-factor authentication when you log in to your online accounts, such as Workday, Gmail and more. The 2FA hardware automatically generates the code and fills it in the field as second factor of authentication.

- **Mobile devices for 2FA:** Mobile devices provide different options for a second factor during the authentication process, such as facial recognition, biometrics and voice recognition. All operating systems, including iOS, Android and Windows, have applications that support 2FA.

  Authenticator apps, such as Microsoft Authenticator and Google Authenticator, eliminate the need to receive code on your mobile device by generating an in-app code that you can enter at the time of login when prompted for a second factor.

- **Passwordless authentication:** With this type of authentication method, the user will receive a push notification on a trusted mobile device that they can approve or deny for granting/denying access to their accounts. Microsoft Authenticator can be used to implement passwordless authentication in your organization.

Beware of social engineering

Social engineering is the art of manipulating, influencing or deceiving someone into sharing confidential information to gain control over their computer system, devices and accounts.

Watch this helpful video from Mastercard to learn more: Exercise Caution Against Phishing

Criminals might use different types of attacks to gain illegal access. Social engineering attacks could look like any of the following:

- Email or text from a friend
- Email or text from a trusted source
- Email or text that creates distrust or a sense of urgency to act

Below are the best practices to defend yourself and your business against a social engineering attack:

- Don't open emails and attachments from suspicious sources, and unsolicited attachments, even from people you know. Instead, uncover full email addresses by right-clicking on a sender's name to view the message properties and reveal details that could show that the email is not from a trusted source.[1]
- Turn off the option to automatically download attachments.[1]
- Verify links through a separate channel. If you're given a link to a website to order or ship something, see if you can find the business on Google Maps or via search. It may not exist. Also, before you submit your personal identifying information (PII) or make a purchase, check a website at https://www.getsafeonline.org/checkawebsite/
- Trust your instincts.[1]
- Keep software up to date.[1]
- Apply additional security practices: See if your email software is able to filter certain types of attachments.[1]
- Consider creating separate multiple user accounts on your computer.[1]
- Avoid cryptocurrency. Getting a request to pay for just about anything in cryptocurrency usually indicates fraud.[2]
- Use multi-factor authentication.[3]
- Beware of tempting offers or emails that want you to rush a decision.[3]
- Beware of communications that ask for a change in payment accounts or sensitive information about your business.[3]
- Keep your antivirus software up to date.[4]
- Regularly back up your data.[3]
- Avoid plugging an unknown USB into your computer.[3]

Source:

1. Using Caution with Email Attachments | CISA
2. What To Know About Cryptocurrency and Scams | Consumer Advice
3. Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA
4. Cyber Security Tips, Facts & Statistics for 2025 | Security.org

Cover blind spots with software patching

Watch this helpful video from Mastercard to learn more: Update Software Regularly

Software patching/updates provide 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 following a patch release. This is quite often the case of security breaches, especially for smaller organizations that do not stay on top of their patch management schedule.

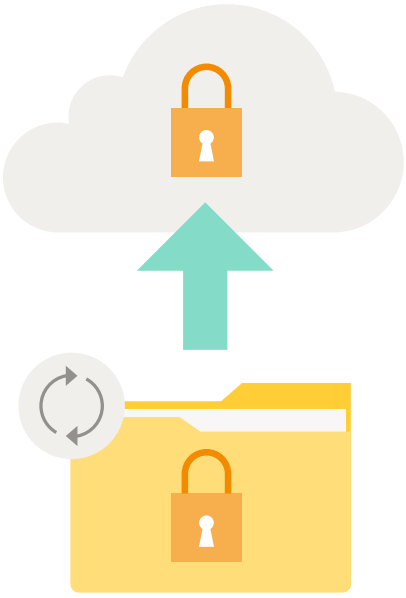
All your business's digital assets (software, operating systems and applications) across computers, phones, printers, routers and more can be used as a weapon against your business if they are not updated (patched) regularly and as soon as they are released.

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.
- Create a culture throughout your business that takes patching seriously.

Back up today for a safer tomorrow

Frequently and 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.



Watch this helpful video from Mastercard to learn more: Back up Data Securely & Regularly

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 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 — including any data that is required to run the business day to day.
  - Back up and secure 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 license 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 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.

Managing data breaches

In 2025, Mastercard commissioned a large research study on small and medium businesses (SMBs) and cybersecurity. The results showed that 39% of U.S. SMBs have experienced a cyberattack. The study also found that U.S. SMBs in the construction industry experienced the fewest cyberattacks of the six industries surveyed (22%). In contrast, the study found that 55% of U.S. professional services businesses experienced a cyberattack, which was the highest of the six industries surveyed.[1]

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 and more) and the consequences of failing to do so are particularly important when you think about your business's online security and the resulting loss of customer trust. 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 damage 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 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(s) from the main network to prevent other devices from becoming 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 can be taken to contain the damage. This includes contacting the local police, financial institutions and credit bureaus (if financial data is compromised), and the U.S. Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) and calling the Cybersecurity & Infrastructure Security Agency (CISA) at 1-844-SAY-CISA or 1-844-729-2472.
5. Notify all individuals whose PII was stolen or otherwise compromised, including customers, employees, suppliers and anyone else who had their PII stolen. Recommend that they change their passwords; monitor their accounts, credit and debit card statements, and credit rating services, such as Experian, Transunion, Equifax and FICO; and freeze their accounts so no one can apply for credit or debit cards or loans in their name.
6. Clean up all traces of the attack by deleting infected/malicious files and moving the deleted files to your computer's trash and then creating 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.
7. Restore systems from backup data to start business as usual.

Source:

1. 2025 Mastercard Proprietary Research: SME Cybersecurity Landscape

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.

Visit the Mastercard Trust Center to access free cybersecurity education, resources and tools designed to help small to medium businesses improve the security of their digital ecosystem and reduce the risk of experiencing a cyberattack. Select the Cybersecurity Learning Journey that best fits your current level of cybersecurity expertise (Learn the Basics, Expand Your Knowledge or Master Your Security).