Cybersecurity assessment report

Developed by Mastercard

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.

SECTION ONE

Why cybersecurity is important 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 cybersecurity knowledge posture. The report also offers strategic recommendations to help you fortify your business's defenses against cyberthreats.

As a business decision-maker, you must protect confidential data and digital assets. Implementing robust cybersecurity processes reduces risks, like untrained staff, outdated software and lost or stolen devices. Let's strengthen your cybersecurity 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 business owners don't take the time to secure their business's digital ecosystem. Cybercriminals know small businesses can be an easy target.

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 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 the 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 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. Fifty-five percent of residents in the U.S. report being less likely to continue doing business with firms that are breached.[1]
- **Legal consequences:** Twenty-four percent of U.S. businesses that experience a cyberattack are subject to lawsuits due to data breaches and other customer impacts, and 15% file for bankruptcy.[2]

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.

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[2]

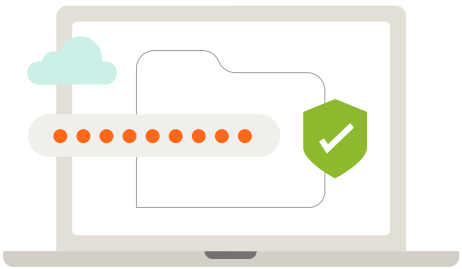
Source:

1. StrongDM: 35 Alarming Small Business Cybersecurity Statistics for 2025

2. 2025 Mastercard Proprietary Research: SME Cybersecurity Landscape — U.S. Report

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. 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 a 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. StrongDM: 35 Alarming Small Business Cybersecurity Statistics for 2025

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

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 systems, 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.

Visit:
GCA Cybersecurity Toolkit Backgrounder: Know What You Have Toolbox

How to Inventory Your Devices, Applications, and Accounts

Cybersecurity awareness and training

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

Watch this helpful video from Mastercard: Educate and train your employees

Recommendation:
This report is a valuable cybersecurity training resource. Download it, share it with your employees, and review each section together in staff meetings to strengthen your business's cyber resilience.

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 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.

SECTION TWO

Authentication and social engineering

Implement strong password guidelines

Passwords are the first line of defense against cyberthreats, and therefore, you should follow these strong 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 uppercase 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 the 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 password 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. Tech Republic: 5 Reasons Why You Should Use a Password Manager

Store, protect and share with password managers

Password managers are tools that provide 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.

Visit passwordmanager.com to learn more about password managers.

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

- No need to memorize multiple passwords
- Increased protection against phishing
- Secure sharing of sensitive information
- Auto-generation of highly secure passwords

Enhance security with two-factor 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 within 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. CISA: Using Caution with Email Attachments
2. Consumer Advice: What To Know About Cryptocurrency and Scams
3. Cybersecurity and Infrastructure Security Agency CISA: Cybersecurity Best Practices
4. Security.org: Cyber Security Tips, Facts & Statistics for 2025

Be mindful of phishing attacks

Phishing is a type of social engineering attack often used to steal user data, including login credentials, personal identifying information (PII) and credit card numbers.

Phishing 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.

Types of phishing attacks:

- **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 business 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. Cyber attackers 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.
- **Business email compromise:** Criminals hack into email systems to gain information about business payment systems, then deceive company employees into transferring money into their bank account
- **Tech support scams:** Fake calls or messages claiming to be from tech support, asking for payment or access to your computer
- **Account takeover:** Fraudsters gain control of a victim's existing accounts, such as banking, email or social media accounts, to steal money or sensitive information

SECTION THREE

Patching, backups, access management and antivirus software

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.

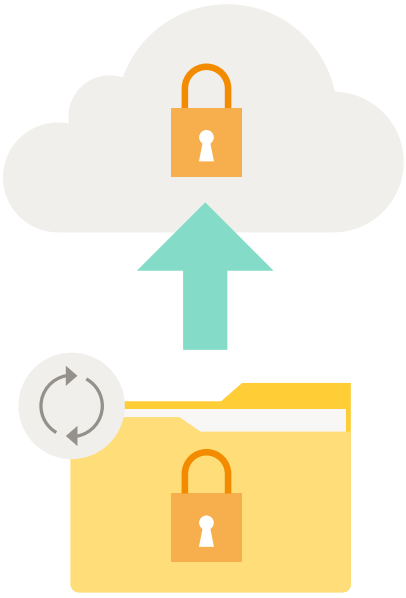
All your business's digital assets (software, operating systems and applications) across computers, phones, printers, routers and more, can be used as a weapon against your business if they are not updated (patched) regularly and as soon as they are released.

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 Personally Identifiable 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, home address, email address, 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.

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. Limiting access helps protect your business from employee mistakes and insider threats.

Watch this helpful video from Mastercard to learn more:
Limit access rights

Evaluate every employee's business needs to access devices, operating systems, software/applications and online accounts. Don't grant log-on 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.

Scan and protect with antivirus software

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

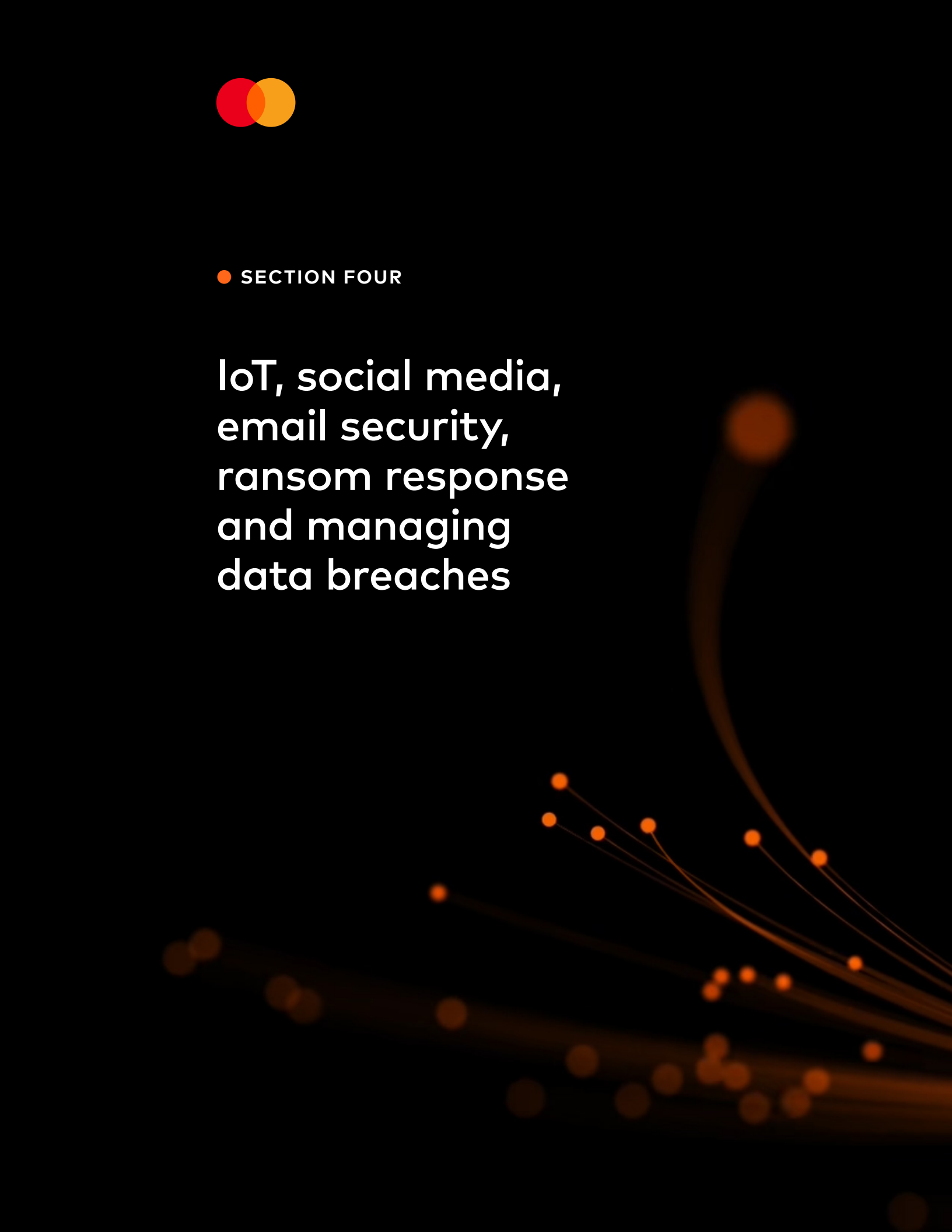
Cybercriminals use software viruses to disrupt systems and cause major operational issues that can result in data loss and leakage.

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: Use anti-virus software

SECTION FOUR

IoT, social media, email security, ransom response and managing data breaches



Enhance security for Internet of Things

To learn more about Internet of Things (IoT) security best practices, visit What is IoT security and top 10 IoT security best practices.

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

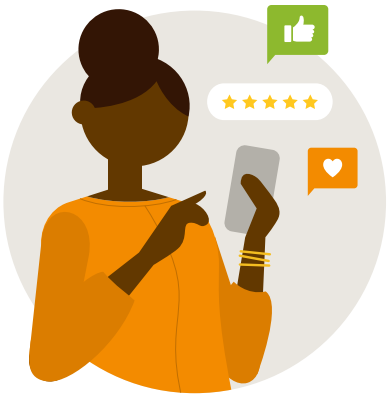
These devices can exchange data with other devices and systems over the internet or other communications networks. Listed below are a few threats associated with IoT devices:

- Vulnerability to attacks: Many IoT devices lack strong security features, making them vulnerable to hacking and cyberattacks
- Data breaches: IoT devices can collect and transmit sensitive data, making them targets for data theft
- Network compromise: A compromised IoT device can serve as a gateway for attackers to infiltrate a larger network
- Operational impact: Cyberattacks on critical IoT devices can disrupt operations and cause significant harm
- Liability: Businesses and individuals can face legal and financial consequences for failing to protect IoT devices

Top five IoT cybersecurity actions:

- Change default passwords: Always replace factory-set usernames and passwords with strong, unique credentials.
- Keep firmware updated: Regularly update device software to patch unknown vulnerabilities.
- Segment your network: Place IoT devices on a separate network from critical business systems to limit exposure.
- Monitor device activity: Use tools to track unusual behavior or unauthorized access attempts.
- Disable unused features: Turn off services like remote access, Bluetooth or ports that aren't needed.

Maintain social media security



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.

Social media accounts come with a variety of risks, especially for businesses and individuals who rely on them for communication, branding or customer engagement.

To learn more about social media security best practices, visit National Security Agency: Keeping Safe on Social Media.

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.

Here are the main categories of risks:

Security risks:

- Account hacking: Weak passwords or phishing attacks can lead to unauthorized access
- Credential stuffing: Attackers use leaked credentials from other breaches to access social accounts
- Malware distribution: Compromised accounts can be used to spread malicious links to followers

Reputation risks:

- Inappropriate posts: Accidental or malicious posts can damage brand image
- Fake accounts: Impersonators can mislead customers or damage trust
- Negative publicity: Controversial posts or responses can lead to viral backlash

Secure your social media accounts:

- Immediately update and frequently review privacy settings
- Protect your location data
- Know your "friends"
- Lock down your privacy settings
- Don't post critical information
- Minimize pivoting to home and work networks
- Be aware of your physical and virtual surroundings
- Secure and strengthen your passwords
- Monitor your cyber footprint
- Report suspicious activities
- Recognize social engineering tactics
- Close the window into your private life

Pump up email 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.

Watch this helpful video from Mastercard: Enhance email filtering

Prepare a ransomware response plan

Learn more about ransomware mitigation steps for businesses. Access the No More Ransom Project's free prevention advice for businesses

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 assigned to develop and communicate a Cyber Incident Response Plan for your business.
- Communication guidelines, including notification details to affected individuals and stakeholders

Learn more about ransomware response plans from the Cyber Readiness Institute, visit the Cyber Readiness Institute's Ransomware Playbook.

Report a ransom attack crime.

Managing data breaches

One in three U.S. small and medium businesses surveyed reported experiencing a cyberattack in 2024, and 71% do not believe their current cyber defenses are mature enough to withstand today's threats.[1]

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, intellectual property and more) and develop a cybersecurity action plan and a cyberincident response plan (see Business Continuity 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 becoming 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 contacting the local police, financial institutions, and credit bureaus (if financial data is compromised). In addition, contact the Federal Bureau of Investigation (FBI) at 1 (800) 225-5324 or report online to the FBI's Internet Crime Complaint Center (IC3) at https://www.ic3.gov. Also, call the U.S. Cybersecurity & Infrastructure Security Agency (CISA) at 1-884-729-2472 or 1-833-SAY-CISA.
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.

Source:

1. Viking Cloud's 2025 SMB Threat Landscape Report: Small and Medium-Sized Businesses, Big Cybersecurity Risks

Free cybersecurity education and resources to help protect your business

- Mastercard Trust Center (Mastercard Trust Center | Cybersecurity Solutions for Every Business)
- Global Cyber Alliance (GCA Cybersecurity Toolkit for Small Business | Sponsored by Mastercard) and (Cybersecurity Courses for Small Business)
- Cyber Readiness Institute (Cyber Readiness Program — Cybersecurity Awareness Training)
- No More Ransom Project (Home | The No More Ransom Project) and (Crypto Sheriff | The No More Ransom Project)

To learn more about ransomware response plans from the No More Ransom Project, visit The No More Ransom Project.

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 and 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).