

Cybersecurity Survival Guide for SMBs

Learn about the most common types of cyberattacks, assess your organization's cyber risk and take five important steps to stop breaches

Table of Contents

Small and Medium Businesses Are Targets	3
SMB Cybercrime by the Numbers	3
How Modern Cyberattacks Evade Legacy Security Technology	4
Five Steps to Protect Your Business from Modern Cyberattacks	5
Step 1: Understand the Reality of Cyberattacks	5
Step 2: Implement Basic Cybersecurity Hygiene Practices	6
Step 3: Train, Test and Support Your Employees	6
Step 4: Invest in Modern Endpoint Protection	7
Step 5: Secure Your Email and Communication Channels	7
Overcoming Limited Resources and Expertise	7

Small and Medium Businesses Are Targets

It's easy to assume cybercriminals only target major enterprises. These large organizations have mountains of valuable and sensitive data across their environments and critical operations that, if disrupted or taken down, can result in millions of dollars in lost revenue and reputational damage.

But while breaches of large organizations make news headlines, small and medium-sized businesses (SMBs) are also at risk. SMBs often lack dedicated cybersecurity teams and may not have the modern cybersecurity software, skills or resources to protect themselves. And SMBs, like larger businesses, hold valuable, sensitive data such as employee and customer records, financial transaction information, intellectual property and access to business finances and larger networks critical to their success.

Cybercriminals recognize both the vulnerability and value of SMBs, viewing them as easy prey, ripe for compromise, ransomware and data theft. As governments and organizations around the globe increase funding for cybersecurity, the market and regulatory pressure to avoid the spotlight continues to mount, making SMBs ideal targets for various threat actors and cybercriminal organizations.

SMB Cybercrime by the Numbers

Cyberattacks always carry significant consequences, but for SMBs they can be devastating.

In 2024, IBM found the average cost of a data breach to an SMB was \$4.88 million USD.¹ Such impact can be more than enough to end the life of a company.

- 50% of SMBs lack the resources or tools necessary to protect their business 24/7²
- 73% of SMB owners and leaders reported experiencing data breaches or cyberattacks in 2023³
- 85% of ransomware attacks targeted SMBs in 2023⁴

Cyberattacks come in many forms, from ransomware and phishing attacks, to the theft of sensitive data such as intellectual property and personal information of employees and customers.

Here are some of the common cyberattacks cybercriminals use to gain access and compromise systems and data:

- **Malware:** Malicious programs and code developed by attackers to manipulate or otherwise compromise computer systems, networks, applications and data
- **Malware-free attacks:** Fileless infections that don't write anything to disk and use built-in tools to move laterally and compromise your environment
- **Vulnerabilities:** Weaknesses in systems or applications that cybercriminals exploit to gain unauthorized access to a computer system
- **Phishing and business email compromise:** Primarily email-based scams that impersonate credible people and organizations to steal credentials or sensitive information
- **Compromised credentials:** Stolen identity and account data (e.g., username and password) used to access systems and networks, masked as legitimate users to perform various attacks
- **Insider threats:** Employees who wittingly or unwittingly misuse, harm or otherwise exploit critical systems, networks or data
- **Zero-days:** Previously unknown vulnerabilities and exploits that attackers leverage in planned and targeted attacks

¹ IBM Cost of a Data Breach Report 2024

² UpCity, [2022 Study: 50% of SMBs Have a Cybersecurity Plan in Place](#)

³ Fortra, [2023 Business Impact Report: Small Businesses and Cyberattacks](#)


⁴ Veeam, [Small Business Ransomware: What You Need to Know](#)

How Modern Cyberattacks Evade Legacy Security Technology

While many SMBs are familiar with malware and may have installed antivirus to combat such attacks, cybercriminals are evolving their strategies to bypass traditional security tools. Many cybercriminals now employ human-engineered methods to break into businesses of all sizes.

For example, 79% of attacks in 2024 were malware-free to evade legacy antivirus software searching for known file- and signature-based malware, according to the [CrowdStrike 2025 Global Threat Report](#). This finding underscores how criminals are using increasingly sophisticated and stealthy techniques tailor-made to evade autonomous detections like those produced by antivirus software.

Once inside a network, cybercriminals can begin moving laterally across your systems and infrastructure, allowing them to compromise your systems and exfiltrate your data in the following ways:

- **Data theft:** When an attacker extracts and then sells valuable employee data or intellectual property
 - **Ransomware:** A type of malware that disables access to your system and data until a ransom is paid
 - **Extortion:** When an attacker extracts and threatens to expose sensitive information on the internet unless the victim makes a payment
 - **Hacktivism:** Intrusion activity undertaken to gain momentum, visibility or publicity for a cause or ideology
- 
- A decorative graphic consisting of numerous thin, parallel diagonal lines in varying shades of gray, creating a sense of motion and depth across the bottom half of the page.

Five Steps to Protect Your Business from Modern Cyberattacks

Follow these steps and associated action items to ensure your business, data and customers are protected from modern cyber threats.

Step 1: Understand the Reality of Cyberattacks

MYTH 1: Cyberattacks are conducted by amateur hackers.

FACT: Malicious cybercriminals — aka “adversaries” — are highly organized and disciplined, and they act fast. CrowdStrike now actively tracks over 255 known adversary groups.

MYTH 2: Cybercriminals don’t care about my data.

FACT: SMBs don’t fly under the radar of cybercriminals. In fact, Mimecast detected an increase in threats targeting small businesses in the first half of 2024.⁵ Sensitive data is valuable, regardless of company size. Moreover, SMBs often lack modern cybersecurity technology and personnel, making SMBs quick and easy targets for attackers. According to the 2023 Hiscox Cyber Readiness Report, 41% of SMBs fell victim to a cyberattack in 2023, a rise from 38% in 2022 and close to double from 22% in 2021.⁶

MYTH 3: Antivirus and a firewall will protect my SMB from cyber threats.

FACT: Traditional antivirus solutions fail to detect modern and malware-free attacks, which make up 79% of cyberattacks.⁷ And while antivirus and a firewall are critical security measures to have in place, they won’t stop a cyberattack that starts with email or text message.

MYTH 4: I’ll know if I’ve been breached.

FACT: Ultimately, yes, at some point you will know you were breached. But it could take weeks or even months before you know you’ve been hit. It takes an average of 194 days to identify a data breach and an average of 64 days to contain it.⁸ And the longer cybercriminals linger in a target environment, the more damage they can inflict.

MYTH 5: My company will bounce back after an attack.

FACT: The process of recovering from a data breach is arduous. Factoring in business downtime, decreased profitability, legal fees and more, severe attacks can cause an SMB to shut down for good.

Action Checklist:

Perform an organizational security assessment. Evaluate your hardware, software, physical security and employee security awareness.

- ☐ Can stolen or lost laptops provide easy data access?
- ☐ Are remote employees’ devices secure from unauthorized family members?
- ☐ Is your office physically secure from unbadged intruders?
- ☐ Do your employees undergo security awareness training?
- ☐ How many employees click on phishing emails?

⁵ [Mimecast Global Threat Intelligence Report 2024 - January-June](#)

⁶ [Hiscox Cyber Readiness Report 2023](#)

⁷ Source: 2025 CrowdStrike Global Threat Report

⁸ [IBM Cost of a Data Breach Report 2024](#)

Step 2: Implement Basic Cybersecurity Hygiene Practices

The following practices can have a huge impact on helping build up your defenses.

- **Perform regular backups of critical data:** On-premises or cloud backups accelerate recovery but may still be at risk if attackers linger undetected.
- **Create a strong password policy:**
 1. Enforce strong, unique passwords updated every 30-90 days.
 2. Implement multifactor authentication (MFA) for critical systems.
 3. Use biometric authentication alongside passwords where possible.
- **Secure physical environments:**
 1. Require employee ID badges.
 2. Lock laptops to prevent theft.
 3. Limit employees' physical access only to areas relevant to their roles.
 4. Train staff on risks like "tailgating" into secure areas.
- **Follow the data:** Map where data enters, moves and is stored. Deploy endpoint security (endpoint detection and response, managed detection and response, or extended detection and response) for real-time protection.
- **Encrypt your data:** Data encryption ensures safety in transit and at rest, protecting data from unauthorized access or tampering.
- **Automate patch updates:** Many of the biggest breaches have started with exploited vulnerabilities. With the proliferation of open source and cloud applications, updating software is critical to ensure you aren't the next victim of a major breach. The [U.S. Cybersecurity and Infrastructure Security Agency](#) (CISA) provides an updated list of all known exploited vulnerabilities.
- **Lock down your cloud environments:** Use strong protections for virtual machines, APIs, workloads and cloud drives.
- **Secure remote access with a VPN:** VPNs safeguard remote employees connecting from personal devices or untrusted networks like airports or cafes.

Step 3: Train, Test and Support Your Employees

Your workforce plays a critical role in your security defenses. Mimecast found that training reduces employee click rates on phishing emails by 25%.⁹

- **Train staff on cybersecurity best practices:** Educate employees on password management, suspicious activity and physical security (e.g., locking devices and properly handling sensitive documents).
- **Test phishing awareness:** Employees should recognize fraudulent emails, URLs and text messages.
- **Evaluate security readiness:** Periodically test employees' ability to respond to phishing attacks, social engineering and malware attempts.
- **Create a comprehensive incident response plan:** Collaborate across leadership and stakeholders to outline clear actions for breaches. Test and revise the plan after incidents to ensure effectiveness.

⁹ [Mimecast Exposing Human Risk Report](#)

Step 4: Invest in Modern Endpoint Protection

Endpoint protection platform (EPP) software offers modern security tools to protect endpoints — including computers, mobile devices, servers and other connected devices — from known and unknown threats and vulnerabilities.

Endpoint protection provides many security benefits, such as:

- Real-time, end-to-end visibility
- Improved threat detection and resolution
- Enhanced efficiency and improved outcomes

EPP has become an imperative component of stopping breaches for businesses and can also help achieve cyber insurance initiatives.

Step 5: Secure Your Email and Communication Channels

Cybercriminals are using AI to deliver more sophisticated threats, often in the form of phishing and business email compromise (BEC). A strong email security strategy uses a layered approach including:

- Pre-filtering to remove known bad emails
- AI including natural language processing (NLP) and machine learning (ML) capabilities to identify suspicious messages
- Protection at the point of detection to prevent threats from reaching employee inboxes

Overcoming Limited Resources and Expertise

When starting up, SMBs are often looking to keep their business data, devices and users safe from cyber threats by using an affordable, easy-to-manage solution to help them achieve those goals.

Protection from Modern Cyber Threats

Every organization faces external threats, like phishing and business email compromise, and internal threats, like data loss. The critical piece that intersects these risks is the human — your employees. Employees can knowingly, or unknowingly, share sensitive data or click a malicious link in a phishing email.

Mimecast provides SMBs with industry-leading human risk management — a simple solution to protect email and collaboration, detect insider risk and empower your employees to be part of your security solution.

[Mimecast Cloud Integrated](#) delivers multi-layered, AI-powered protection across email and collaboration security, DMARC enforcement, security awareness training, and data backup and recovery. Organizations benefit from its out-of-the-box configuration, simplified administration and five-minute deployment.

CrowdStrike provides modern cybersecurity solutions to give small businesses enterprise-level protection and peace of mind that their growing business is safe from threats. [CrowdStrike Falcon® Go](#) offers small businesses next-generation antivirus, device protection, express support, and accessible, manageable and affordable cybersecurity to meet any budget. And once a business increases in size and complexity, [CrowdStrike Falcon® Complete Next-Gen MDR](#) provides 24/7 protection and elite expertise powered by the AI-native CrowdStrike Falcon® platform. Operating as a seamless extension of customer teams, Falcon Complete Next-Gen MDR delivers expert platform management, monitoring and advanced threat detection, investigation and response across all key attack surfaces including endpoint, cloud and identity.

Together, Mimecast and CrowdStrike are protecting SMBs against modern cyber threats.

About CrowdStrike

[CrowdStrike](#) (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches



About Mimecast

Mimecast is an AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.

Contact Mimecast