



eBook

Cybersecurity Survival Guide for Small and Medium Businesses

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

Presented by:



Table of Contents

Small and Medium Businesses Are Targets 3

SMB Cybercrime by the Numbers 3

How Modern Cyberattacks Evade Legacy Security Technology 4

Four 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 and Continuously Test Employees 7

Step 4: Invest in Modern Endpoint Protection 7

Overcoming Limited Resources and Expertise 7

Protection from Modern Cyber Threats 7

Complete Protection, Managed for You 8

SMBs Trust CrowdStrike to Keep Them Secure 9

Protect Your Business with CrowdStrike Falcon Complete Next-Gen MDR 10

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. An SMB often lacks a dedicated cybersecurity team, and it may not have the modern cybersecurity software, skills or resources to protect itself. And SMBs, like larger businesses, also 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 to SMBs they can be devastating.

In 2024, IBM found the average cost of a data breach to a small business 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 the past year³
- » 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.



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

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](#)

Below are some of the common attacks cybercriminals use to gain access and compromise your 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 and applications that cybercriminals exploit to gain unauthorized access to a computer system
- » **Phishing:** 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 and 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

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. Now, many cybercriminals employ human-engineered methods to break into businesses of all sizes.

According to the [CrowdStrike 2024 Global Threat Report](#), 75% of attacks are malware-free to evade legacy antivirus software searching for known file and signature-based malware.

This finding underscores how criminals are using increasingly sophisticated and stealthy techniques tailor-made to evade autonomous detections like those produced by antivirus software.



**According to
CrowdStrike's 2024
Global Threat
Report,
75% of
attacks are
malware-free to
evade legacy
antivirus software
searching for
known file- and
signature-based
malware.**

Once inside the network, cybercriminals – or adversaries, as CrowdStrike refers to them – 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 an extortion payment
- » **Hacktivism:** Intrusion activity undertaken to gain momentum, visibility or publicity for a cause or ideology

Four Steps to Protect Your Business from Modern Cyberattacks

Step 1: Understand the Reality of Cyberattacks


MYTH 1: Cyberattacks come from amateur hackers.

FACT: Malicious cybercriminals, or adversaries, are highly organized, disciplined and act fast. In fact, CrowdStrike now actively tracks over 245 adversary groups.

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

FACT: SMBs don't fly under the radar of cybercriminals. 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 the 2022 report and close to double from 22% in 2021.⁵

MYTH 3: Antivirus and a firewall will protect my SMB from cyber threats. **FACT:** Antivirus is designed to identify and stop viruses and malware; however, it's incapable of detecting and stopping sophisticated techniques employed by today's attackers. For example, traditional antivirus solutions won't detect attacks that are malware-free or that involve the use of valid identity credentials that have been stolen, which now make up 75% of attacks. Cybersecurity tools are a major component of an effective defense, but you also need modern processes and people to run them.



Once inside the network, cybercriminals — or adversaries, as CrowdStrike refers to them — can begin moving laterally across your systems and infrastructure, allowing them to compromise your systems and exfiltrate your data.

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

FACT: Ultimately, yes, at some point this is true, you will know you were breached. But it could take weeks or even months before you know you've been hit. The IBM Cost of a Data Breach Report 2024 found that it takes an average of 194 days to identify a data breach and an average of 64 days to contain it.⁶ 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 even cause SMBs to shut down for good. In a 2024 TechValidate survey of SMBs, 33% of respondents said they would "likely" or "definitely" go out of business if they experienced a cyberattack.⁷

Step 2: Implement Basic Cybersecurity Hygiene Practices

The following practices don't cost any money and can have a huge impact on helping build up your defenses.

- » **Create a strong password policy:** Never share passwords or use the same password for multiple applications, cloud apps or servers. Managing passwords will allow you to watch for suspicious behavior and shut down access if needed.
- » **Enforce multifactor authentication (MFA):** MFA requires a password and a token to access your critical applications, adding an important layer of protection. Google, Symantec and Microsoft all offer free authentication tools and seamlessly connect popular apps.
- » **Perform regular backups of critical data:** Whether on-premises or in the cloud, having a backup of your data will help you recover faster in the event of a breach. However, your backups could be encrypted if criminals have had access to your systems without your knowledge. While backups are essential, it's far more important to establish a resilient defense upfront.
- » **Keep current with software patches and security 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 are not 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:** Protect your cloud drives (such as Box or Google Drive) by implementing MFA and adhering to the principle of least privilege, which ensures employees only have access to the resources they need for their jobs.
- » **Implement and test your threat detection and response:** Make time to analyze your environment and user behaviors for malicious or abnormal activities. Stay current on threat actors, tradecraft and indicators of attack. Define, document and test what a successful incident response looks like.
- » **Secure your network:** Create a private VPN and keep your WiFi secure and hidden. Make sure to look for suspicious behavior and access points. This is essential for any business with remote employees and should be available at no additional charge from your internet service provider.

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

7 TechValidate survey of Falcon Go customers, April 2024, n=143. For more data, see this CrowdStrike blog post: "[3 Ways Small Businesses Can Make Big Strides in Cybersecurity](#)," June 14, 2024.

Step 3: Train and Continuously Test Employees

Educate your employees: Your entire workforce should be aware of the types of security threats and social engineering attacks they face at work, such as phishing, smishing, honey trapping and more. For definitions and tips, check out [10 Types of Social Engineering Attacks](#).

Test and evaluate your employees' ability to identify fraudulent messages: Many breaches start with an employee falling for the bait of a phishing attack. Teaching your employees how to identify suspicious emails, URLs, text messages and other phishing signs is critical to preventing a breach.

For more guidance, visit [How to Create an Employee Cybersecurity Awareness Training Program](#).

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 response	Enhanced efficiency and improved outcomes
----------------------------------	--	---

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

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

CrowdStrike offers SMBs next-generation antivirus, providing an accessible, manageable and affordable security solution.

But once a business increases in size and complexity, it may need to bring on expert resources to manage more complex cybersecurity needs, or invest in a fully managed solution that is operated on its behalf. And while EPP solutions provide autonomous protection, they still require a dedicated team to set policies and monitor, respond to and stop attacks.

Many SMBs simply don't have the budget or time to find, hire and pay for these resources 24/7. If this sounds like you, a managed detection and response (MDR) solution may be the best fit for your business.

MDR is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring and response.

Managed detection and response (MDR)

MDR is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring and response.

Complete Protection, Managed for You

[CrowdStrike Falcon® Complete Next-Gen MDR](#), CrowdStrike's industry-leading MDR service, provides 24/7 protection and elite expertise powered by the AI-native CrowdStrike Falcon® platform. Operating as a seamless extension of a customer's team, 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.

Falcon Complete Next-Gen MDR is designed to solve the unique security challenges SMBs face. It provides a fully managed security service that removes the burden of cybersecurity from internal teams and delivers the same level of protection used by the world's largest organizations. With Falcon Complete Next-Gen MDR, SMBs gain access to a dedicated team of cybersecurity experts who handle everything from threat detection to active response and remediation, ensuring that businesses are protected around the clock.

This managed security solution leverages the power of CrowdStrike's Falcon platform, which uses AI-driven technology to detect and stop even the most advanced cyberattacks. Falcon Complete Next-Gen MDR goes beyond detection by providing end-to-end threat remediation, allowing SMBs to stay focused on their core operations without worrying about cyber incidents. Scalable and cost-effective, Falcon Complete Next-Gen MDR is built to grow alongside SMBs, offering enterprise-grade protection tailored to their size and needs. Falcon Complete Next-Gen MDR delivers the expertise, technology, and proactive protection SMBs require to safeguard their business without the complexity of managing it themselves.

With quick deployment and an immediate expansion of your security team, the benefit is felt in days, not months. Gain actionable insights and consistent reporting for an immediate ROI.

- » Saves over 2,500 hours per year from a reduction in security incidents⁸
- » Provides the equivalent of five expert operations center analysts and five elite human threat hunters⁹
- » Have peace of mind with the CrowdStrike Breach Prevention Warranty, provided at no additional cost¹⁰



According to Gartner, by 2025, 50% of organizations will use MDR services for threat monitoring, detection and response functions.



"Falcon Complete lets me sleep far better at night."

Customer quoted in Forrester Consulting's

["The Total Economic Impact™ of CrowdStrike Falcon Complete"](#)

8 Forrester Consulting, ["The Total Economic Impact™ of CrowdStrike Falcon Complete"](#)

9 Forrester Consulting, ["The Total Economic Impact™ of CrowdStrike Falcon Complete"](#)

10 Disclaimer: The breach prevention warranty is not available to all customers, in all regions. See [FAQ](#) for exclusions.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Attribution: Gartner, Market Guide for Managed Detection and Response Services, Pete Shoard, Craig Robinson and others, October 25, 2021.

SMBs Trust CrowdStrike to Keep Them Secure

Customer Story 1

Company: Central National Bank of Waco

Industry: Banking

Number of Endpoints: 200

Challenges:

- » Reactive, labor-intensive cybersecurity strategy
- » Manual threat management
- » High cost of cybersecurity services

Solution:

CrowdStrike Falcon Complete Next-Gen MDR delivers comprehensive managed detection and response (MDR) for endpoints, identities, cloud workloads and more.

Business Outcomes:

- » Improved visibility into security operations
- » Instilled confidence in customers' asset protection
- » Reduced mitigation time from two days to seconds

Read the full case study [here](#).

Customer Story 2

Company: Commercial Bank of California

Industry: Banking

Number of Endpoints: 550

Challenges:

- » In light of heightened ransomware risk, CBC needed modern endpoint security to replace its legacy tools
- » CBC also needed robust cloud security to protect its growing public cloud infrastructure
- » With a lean IT and security team, the bank needed managed detection and response to provide 24/7/365 security

Solution:

CBC licensed the CrowdStrike Falcon platform along with several product modules and services, including CrowdStrike Falcon® Insight XDR for extended detection and response, CrowdStrike Falcon® Cloud Security, CrowdStrike Falcon® Identity Protection and CrowdStrike Falcon Complete Next-Gen MDR for 24/7 managed detection and response.

Business Outcomes:

- » Zero breaches with CrowdStrike
- » 34% reduction in cyber insurance premiums
- » 24/7 managed detection and response with unified security from endpoint to workload

Read the full case study [here](#).



“CrowdStrike performed as if I had someone onsite 24/7 monitoring our assets all the time, even at three o’clock in the morning. It gives me the ability to go home and relax.”

Rusty Haferkamp CISO,
Central National Bank of Waco



“While the previous vendor claims to be MDR, they simply alert us if they detect a threat and guide us on the remediation. In contrast, Falcon Complete will try to remediate the threat before escalating it.”

Kevin Tsuei SVP
Information Security
Officer, CBC

Protect Your Business with CrowdStrike Falcon Complete Next-Gen MDR

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.**

Learn more: <https://www.crowdstrike.com/>

Follow us: [Blog](#) | [X](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)