Cybersecurity for Small Businesses

Discover the latest cyber threats and how to protect your organization

First Citizens Bank

Safeguarding your business

Cybercriminals are setting their sights on small and medium-sized businesses, or SMBs, unleashing a barrage of cyberattacks designed to infiltrate systems and wreak havoc. According to BlackFog's 2023 Cybersecurity Risk Management Report[1], 61% of SMBs surveyed experienced a cyberattack in the previous year. These weren't one-off attacks, either—87% reported experiencing two or more successful attacks during that year.

While you may think hackers would prefer to target corporations with vast amounts of data and deep pockets, the reality is that SMBs are highly appealing targets for cybercriminals. Not only do most have valuable data—such as customer payment information—but many lack the level of cybersecurity defenses employed by larger companies.

These combined factors create a risky situation. Thankfully, it doesn't take deep technological knowledge or extensive resources to bolster your defenses. By understanding the key threats and addressing cybersecurity vulnerabilities, you'll be able to better safeguard your business.

Page

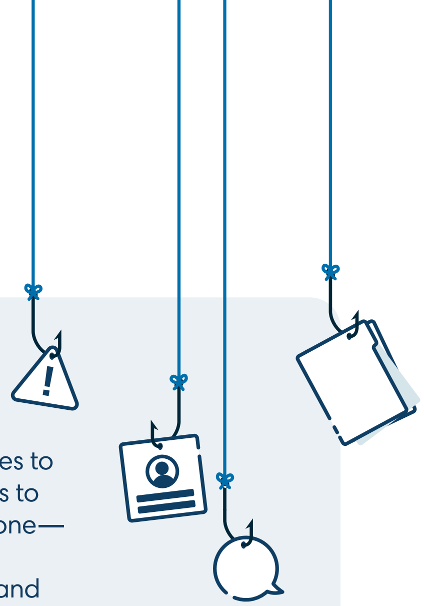
Top cybersecurity threats

Cybersecurity threats come in many forms and occur through various methods. Here are the most common types of cyberattacks targeting small businesses.

Phishing

More than 90% of all cyberattacks begin with a phishing attempt, according to the US Cybersecurity & Infrastructure Security Agency.[2] Based on data compiled by Cisco,[3] 86% of businesses have had at least one employee fall prey to a phishing link.

What is phishing?



Phishing attacks—when a hacker tries to dupe someone into providing access to information via email, text or telephone—are one of the oldest and most well-known threats targeting businesses and consumers. Criminals typically employ phishing schemes to steal login credentials, harvest sensitive information or deceive employees into installing malware. Information stolen through a phishing scheme is also often used to perpetrate future attacks.

Learn more about phishing

Spear phishing

While phishing campaigns cast a wide net, spear phishing is a more targeted attack under the category of social engineering. Attackers thoroughly research targets on social media to gather background information, allowing them to craft highly convincing emails or texts that appear to come from trusted senders like colleagues. Even the most vigilant can be deceived, making this a particularly dangerous cyberthreat for businesses.

Malware

According to the BlackFog report, half of security leaders cite malware attacks as their biggest cybersecurity fear—and rightfully so, given how disruptive these attacks may be. Malware attacks typically begin with an email containing a link or attachment containing malicious software. Once installed, this software can enable criminals to spy, steal company intel, obtain sensitive data or commit fraud.

Ransomware

Panda Security data shows that 46% of SMBs have experienced at least one ransomware attack.[4] Like with malware attacks, a criminal will trick an employee into installing malicious software. Once installed, the software will render a business's data and files unusable, and criminals will hold this data hostage in exchange for money. For SMBs, ransomware attacks may be quite costly. Of those that decided to pay a ransom, 43% surrendered $10,000 to $50,000, and 13% paid more than $100,000.

Learn more about business email compromise

46%
of SMBs have experienced at least one ransomware attack.
Panda Security[4]

Business email compromise

Business email compromise is another type of social engineering attack that involves a person manipulating or tricking an employee into sharing sensitive data or sending funds. SMBs are particularly vulnerable to these attacks. According to the cybersecurity firm Barracuda Networks,[5] businesses employing fewer than 100 people will experience 350% more social engineering attacks than larger companies.

Insider attacks

This type of cybersecurity threat involves employees, contractors or stakeholders either purposely or inadvertently using their authorized access to cause harm to a business.[6] In some cases, the employee might be unaware that their credentials have been stolen and used for criminal purposes.

Cybersecurity vulnerabilities

While cyberattacks differ in approach, they all stem from a common set of cybersecurity vulnerabilities criminals seek to exploit.

Lack of awareness

According to a 2022 CNBC Small Business survey,[7] 6 in 10 business owners say they don't think they'll be the victim of a cyberattack. Many assume that they're too small to target or that their business simply doesn't have any data that would interest hackers. However, cybercriminals often prey on SMBs precisely because so many underestimate the threat.

Limited resources

Unlike large organizations, many SMBs don't have an in-house IT team at their disposal. In fact, almost half of businesses with fewer than 50 employees lack a dedicated cybersecurity budget, according to the 2022 Risk Insights Index conducted by Corvus Insurance.[8] As a result, the burden of cybersecurity often falls on small business owners themselves—and 25% of them admit that they don't have the bandwidth to devote to cybersecurity, according to a 2023 report from Digital Ocean.[9]

Fewer safeguards

Another significant vulnerability is a lack of knowledge. According to the BlackFog report, 39% of business owners say they don't adequately understand the challenges posed by cybercrime. Because many are short on time and knowledge, SMBs often lack essential safeguards like antivirus software, password security protocols and multifactor authentication, or MFA.

Lack of employee training

No formal employee training can also leave many SMBs vulnerable to cyberattacks. Employees are often a company's first line of defense against fraud and cybersecurity threats, underscoring the importance of education. When businesses don't train their employees on cybersecurity best practices, employees may be more easily fooled by the increasingly sophisticated scams criminals employ.

Cybersecurity tip

Criminals often establish an extreme sense of urgency to ensure their target feels pressured to take action before thinking through the request. As a result, one of the most effective fraud prevention tactics small business owners can employ is to encourage employees to slow down, assess the situation and take the time to verify any questionable requests.

Small businesses experience 350% more social engineering attacks than larger companies.

Barracuda Networks[5]

The cost of a cyberattack

It's no secret that a cyberattack can be incredibly disruptive and costly. According to BlackFog, nearly 4 in 10 businesses lost customer data following a cyberattack, while 58% suffered from business downtime.

For companies with less than 500 employees, the average cost of a data breach was $3.31 million in 2023, according to IBM's annual Cost of a Data Breach Report. That's an increase of 13.4% over the previous year.[10]

Beyond the quantifiable financial burden associated with lost or exposed data, cyberattacks often result in reputational risk, which can be just as harmful to a business. According to BlackFog, nearly 1 in 3 companies lost business following a cyberattack. And according to the National Cybersecurity Alliance,[11] 60% of small businesses that experience a data breach permanently close within 6 months of the attack.

$3.31 million

The average cost of a data breach for companies with less than 500 employees

IBM[10]

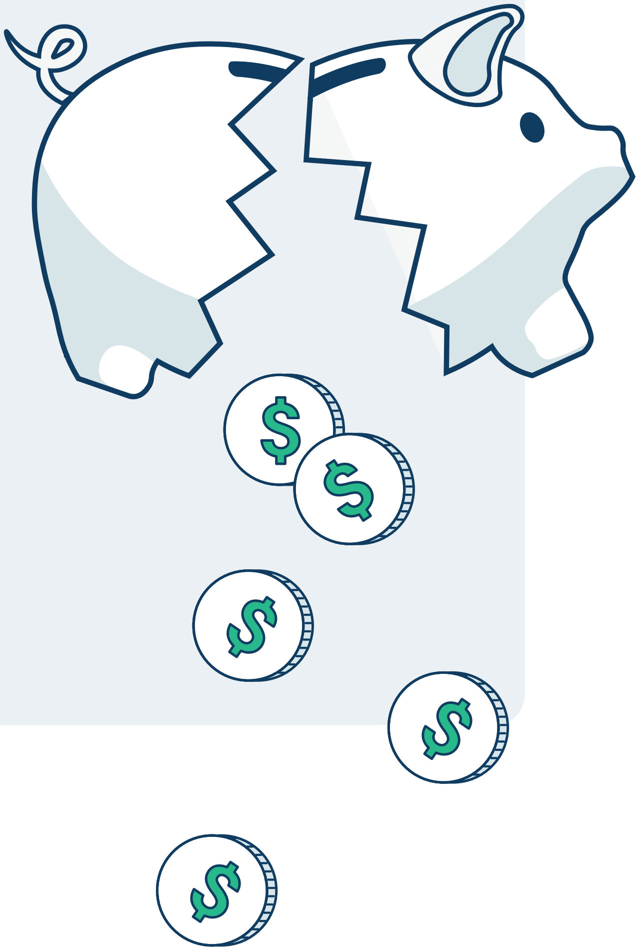
The financial impact

When a data breach occurs, the affected company must immediately take steps to:

- Secure its systems
- Divert resources to data recovery efforts
- File reports with local or national law enforcement
- Investigate the incident
- Communicate the news to customers

The associated expenses—which often include legal support, forensics, data recovery assistance and public relations support—can be extensive.

Learn more about data breaches



Creating a cybersecurity plan

When it comes to cybersecurity for small businesses, planning is an essential first step. A well-structured plan can help you identify cybersecurity vulnerabilities, establish protective measures and educate employees on best practices.

While your small business cybersecurity plan should be tailored to your business, your industry and the types of data you collect, make sure it includes the following components.

95%

of all cybersecurity events can be traced to human error.

World Economic Forum[12]

Employee training

According to the World Economic Forum, 95% of all cybersecurity events can be traced to human error, underscoring the importance of employee education.[12] Conduct regular employee training sessions focused on cybersecurity best practices and key threats. By teaching employees how to spot common red flags and respond properly, you can more effectively safeguard your business.

Cybersecurity awareness training is more than just a one-and-done exercise. It's an ongoing commitment to keeping your data and finances safe. Ideally, fraud awareness training should be part of every new employee's orientation. Likewise, additional training sessions should be held regularly—at least once every 6 months is ideal.

Learn more about cybersecurity awareness training

BYOD policy

Create a bring-your-own-device policy that includes security measures for employees accessing company information on their own phones or laptops.

Remote work policy

Your remote work policy should clearly outline cybersecurity best practices and protocols so company data isn't vulnerable when employees are working outside the office. Specify required precautions regarding unsecured Wi-Fi networks, file sharing and other risks.

Password policy

Implement a robust policy that outlines best practices for password management, establishes minimum password difficulty requirements and requires the use of multifactor authentication and periodic password changes.

Data breach response plan

A data breach response plan that identifies what needs to occur and who's responsible for overseeing these tasks is essential for every business. Your plan should include any outside support that may be required, such as legal, cybersecurity or crisis management consultants. As you develop your data breach response plan, you should also evaluate the benefits of cybersecurity insurance.

Explore the benefits of cybersecurity insurance

Technical safeguards

To help your business reduce vulnerabilities, consider the following tools and technologies as part of your overall cybersecurity plan.

- **Antivirus software:** Choose programs that are designed to protect businesses from sophisticated cyberattacks.
- **MFA:** This provides an extra layer of security by requiring employees to verify their credentials and identity.
- **Virtual private network:** The use of a virtual private network, or VPN, creates a secure connection between employee devices and the company network.
- **Encryption:** Use encryption to keep your customer data safe in the event of a data breach.

Cybercrime presents a very real problem for small businesses, and the problem isn't going away. To help protect your business, create a comprehensive cybersecurity plan, make technological changes to boost your company's digital defenses and train employees to identify and respond to threats.

Learn more in our guide to creating a cybersecurity plan

Sources

[1] Risk Management Report for SMB Cybersecurity Leaders. October 6, 2023. BlackFog. https://privacy.blackfog.com/wp-content/uploads/2023/10/Cybersecurity_Risk_Whitepaper.pdf

[2] Stop Ransomware. US Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/stopransomware/general-information

[3] Cyber Security Threat Trends: Phishing, Crypto Top the List. 2021. Cisco. https://learn-cloudsecurity.cisco.com/umbrella-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

[4] Seventy-three Percent of SMBs Pay Up After a Ransomware Attack. March 27, 2023. Panda Security. https://www.pandasecurity.com/en/mediacenter/smbs-pay-ransomware-attack/

[5] Spear Phishing: Top Threats and Trends. March 2022. Barracuda Networks. https://assets.barracuda.com/assets/docs/dms/Spear-phishing-vol7.pdf

[6] Defining Insider Threats. US Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

[7] Small Business Index Q2 2022. CNBC/Survey Monkey. https://www.surveymonkey.com/curiosity/cnbc-small-business-q2-2022/

[8] Survey Findings: SMB Cyber Readiness. 2021. Corvus Insurance. https://insights.corvusinsurance.com/cyber-risk-insight-index-q1-2022/survey-findings-smb-cyber-readiness

[9] Small Businesses and Cybersecurity: How Startups and SMBs are Viewing Security Threats in 2023. Digital Ocean. https://www.digitalocean.com/reports/cybersecurity-smbs-2023

[10] Cost of a Data Breach Report 2023. IBM Security. https://www.ibm.com/downloads/cas/E3G5JMBP

[11] 60% of Small Companies That Suffer a Cyber Attack are out of Business Within Six Months. March 24, 2017. The Denver Post. https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

[12] The Global Risks Report 2022, 17th Edition. 2022. World Economic Forum. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Disclosures

This information is provided for educational purposes only and should not be relied on or interpreted as accounting, financial planning, investment, legal or tax advice. First Citizens Bank (or its affiliates) neither endorses nor guarantees this information, and encourages you to consult a professional for advice applicable to your specific situation.

Third parties mentioned are not affiliated with First-Citizens Bank & Trust Company.

Links to third-party websites may have a privacy policy different from First Citizens Bank and may provide less security than this website. First Citizens Bank and its affiliates are not responsible for the products, services and content on any third-party website.

First Citizens Bank is a Member FDIC and an Equal Housing Lender ⌂.

NMLSR ID 503941

First Citizens Bank

firstcitizens.com