June 07, 2022

Top 5 Cybersecurity Threats for Small Businesses

Rodika Tollefson
Freelance writer and journalist

SUMMARY

From ransomware to data breaches, small-business owners need to be aware of the biggest cybersecurity threats out there.

Trends such as digital transformation are increasing businesses' reliance on data and digital tools. But for many small and medium businesses implementing technology solutions, securing those tools and data is the top challenge.

A 2021 survey by SMB Group of 761 North American decision makers at small and medium businesses shows that 40% expressed concerns about cybersecurity, more than any other issue. This indicates cybersecurity is at the top of small-business leaders' minds, but addressing it may feel too overwhelming.

John Wilson, senior threat researcher at data security company Agari by HelpSystems, says small and medium companies are a target of opportunity for cybercriminals. It's the lack of cybersecurity measures and resources to defend and remediate attacks that makes these businesses attractive.

"Smaller organizations tend to be more vulnerable and with the scope of cyberattacks no less varied or devastating, they often find themselves the victims," he says.

The first step to defending your business is to understand the threats you face. Here are the five most common cyber threats you need to know.

1. Ransomware

The threat of ransomware, a form of malicious software that prevents access to your data and systems, grew rampant in recent years. Cybersecurity company SonicWall recorded 623.3 million ransomware attacks on its customers in 2021—a 105% increase from 2020 and nearly triple 2019 volumes.

In the past, cybercriminals demanded ransom to restore access to the victim company's data or computers. Many security experts don't recommend paying the ransom because it doesn't guarantee you'll get your access back. More recently, ransomware attacks have evolved into double extortion schemes, with the attackers also stealing sensitive data and threatening to leak it if the victim doesn't pay.

“Ransomware enables significant economic gain for criminals,” says Matt Hartley, co-founder of BreachRX, which provides solutions for privacy incident readiness and response. “The successes that adversaries have had are leading them to more frequently exfiltrate data to exploit for increased ransoms.”

One of the best practices is to have multiple backup versions stored in different media and separate locations that aren't connected to your systems. This ensures you can restore critical systems and data faster in the event of an attack.

2. Insider Threats

Employees, contractors, business associates and other insiders who have or had access to your systems pose either an intentional (malicious) threat or unintentional (such as employees making an accidental error or acting carelessly or negligently). A 2022 World Economic Forum survey of 120 global leaders found that after ransomware and social engineering, malicious insider activities was the type of cyberattack that concerned leaders the most.

Insiders who have access to critical systems are especially a concern, says Curtis Dukes, executive vice president and general manager at the Center for Internet Security (CIS), a global nonprofit recognized for establishing best practices such as the widely used CIS Controls.

“Adversaries such as criminal networks target employees whose credentials can get them access to the infrastructure so they can open multiple ingress and egress points and operate as a privileged user to get certain type of information,” Dukes says.

Techniques for protecting against insider threats include limiting access to data and systems based on role, and logging and monitoring your user behavior for unusual patterns such as downloading large amounts of data or accessing applications they don't need for their job.

3. Misconfigured and Unpatched Systems

Related to insider threats, misconfigured and unpatched systems are often the result of human error or oversight. Cybercriminals exploit weaknesses in these systems to gain access into your network or steal sensitive information. Numerous data breaches in recent years were the result of misconfigurations or software vulnerabilities that had patches available but not applied.

One area that small businesses particularly overlook is web applications, according to Dukes. (CIS considers web application hacking as one of the top five types of attacks). Usually provided by a vendor, a web application can be anything from a shopping cart to a customer portal.

“Typically, organizations don’t patch those at the same frequency as they do operating systems,” Dukes says. “Vendors often issue patch updates for their applications and then it’s incumbent on you to download and install those updates.”

4. Business Email Compromise

Business email compromise (BEC) is a sophisticated scam that impersonates a legitimate person or company to perpetrate fraud, typically in the form of large wire transfers. Less common, BEC

scams have also been used to steal sensitive data, such as employee records. A global survey of 600 companies by cybersecurity company Proofpoint found that 77% faced BEC attacks in 2021.

Cybercriminals often perpetrate these schemes by stealing login credentials through social engineering and phishing. But they can also spoof email addresses, especially if the company doesn't use email security protocols such as DMARC (domain-based message authentication reporting and conformance). Small and medium businesses are particularly susceptible to BEC scams because of cyber defense costs, according to the FBI.

Wilson says attackers may start a BEC scheme by impersonating an executive to contact an accounts receivables employee and request a list of customers who owe company money, including the amounts and dates due. "Now the attackers are armed with a list of dozens or hundreds of possible targets, and all they have to do is trick one into wiring money to a different bank account," he says.

Educating employees about social engineering and phishing threats, as well as implementing additional approval protocols, are low-cost and low-tech ways to help prevent BEC attacks.

> An incident response plan helps you react to a cyber breach, and not only getting back online but also communicating your messaging and notifying authorities. [...] Make sure you're periodically exercising that plan.
>
> *—Curtis Dukes, executive vice president and general manager, The Center for Internet Security*

5. Data Breaches

A data breach is a cybersecurity incident with a confirmed disclosure of sensitive data to an unauthorized party. A quarter of 417 small businesses surveyed by the Identity Theft Resources Center in 2021 experienced a data breach within the past year and 54% within the past one to two years. As a result, many had to take on new debt, dip into cash reserves or use existing loans and lines of credit to pay for the breach.

While protecting against data breaches requires implementing several layers of security measures, following basic cyber hygiene and best practices can greatly boost your data security.

Ways to Improve Your Overall Cyber Defenses

Wilson, of Agari by HelSystems, says the best starting point for defending against common threats is by cataloguing everything of value to your business and then assessing what are the most harmful effects. This enables you to add security measures based on your highest risks.

“Ask yourself, what’s the event that would end our business—that’s obviously the highest priority, while something that would cause 24-hour outage is a lower one,” he says. “It’s really about understanding your business’s digital assets and all the different avenues that those assets could be stolen, compromised, or used against you.”

For very small companies, BreachRx’s Hartley recommends asking existing vendors, such as internet service providers, what security tools may be already available as part of their service. Additionally, he says, invest in basic cyber hygiene, such as password managers and multi-factor authentication.

“If you have a lot of accounts or several hundred employees and it’s overwhelming, start with your executive staff, security team and administrators—the people who have privileged access to systems and decision-making authority related to money,” he says.

Dukes recommends focusing on the core areas identified by the CIS, such as patching vulnerabilities, properly configuring all your devices and other assets (CIS offers free lists of configuration benchmarks), implementing an employee awareness and training program, and creating an incident response plan.

“An incident response plan helps you react to a cyber breach, and not only getting back online but also communicating your messaging and notifying authorities,” he says. “Make sure you’re periodically exercising that plan.”

A common mistake that small businesses make, according to Hartley, is not building security into other business processes proactively.

“Most people don’t think about putting security in at the beginning of building out their technology, or their offering or their business,” he says. “Thinking about security from the beginning is a very clear way to prepare ahead of time and truly reduce the risk.”

Photo: American Express