CLARK SCHAEFER
BUSINESS ADVISORS

CYBERSECURITY

A CEO's guide to cybersecurity

When it comes to cybercrime prevention, the buck stops with the CEO

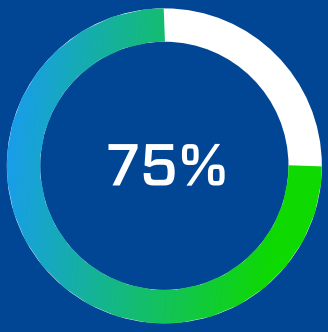
As a CEO, you play one of the most important roles in preventing a cyberattack targeted at your company. Your attitude toward and involvement in cybersecurity can be a critical line of defense against a cyberattack – only if you're making the right decisions.

Far too many CEOs take a distanced approach, however, leaving the organization's cybersecurity strategy in the hands of their IT professionals. There's no question your cybersecurity plan requires assistance from IT for operational and technical responsibilities, but it's your responsibility to make it a priority and give it the attention it deserves.

P.S. The courts have set precedent for holding the CEO and board of directors accountable for cybersecurity. Gartner estimates that up to 75% of CEOs could be held personally liable for data breaches by 2024[1].

Small and medium-sized business (SMBs) CEOs typically have a lot on their plates with limited resources and rapidly changing priorities. But none of that will matter if company data is held for ransom, customer information is leaked or confidential intelligence is stolen. Even more troubling is the pervasive myth that smaller companies are not as vulnerable to a cyberattack.

A cyberattack has the potential to destroy your business, making it a complex risk that needs to be addressed by company leadership.



Up to 75% of CEOs could be held personally liable for data breaches by 2024.

[1] https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl

[2] Ponemon Institute, 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses, October 2019

[3] https://www.prweb.com/releases/new_study_reveals_one_in_-three_smbs_use_free_consumer_cybersecurity_and_one_in_five_use_no_endpoint_security_at_all/prweb16921507.htm

SMBs ARE vulnerable to cybercrime

Large-scale cyberattacks like Solar Winds and Colonial Pipeline make international headlines. But the bigger organizations aren't the only ones at risk for devastating breaches.

A recent study from the Ponemon Institute indicated that 63% of SMBs worldwide experienced a data breach during fiscal year 2019[2]. Another study found that 43% of small businesses lack a cybersecurity plan[3]. Hackers examine the trends too. They know where to hit SMBs to exploit gaps in security.

Limited resources + growing threats = greater risk for SMBs

SMBs often have fewer resources to devote to cybersecurity—a 2017 study published by the Better Business Bureau (BBB) found that 28% of SMBs cited a lack of resources as their top obstacle to achieving cybersecurity goals. In addition, 27% of SMBs said that they lack the necessary expertise in house to achieve their goals.

Additionally, the threat landscape is more complex, with cyberattacks taking on many forms. We hear a lot about phishing attacks, data breaches, and ransomware. These common cybercrime tactics become more sophisticated as businesses get better at fighting them.

So, what actions can CEOs take to define their company's cybersecurity posture and protect it from a threatening landscape? The answer is leveraging technology, people and processes to build a cybersecurity framework that can reduce the risk and severity of an attack.

Common Cyberthreats to Small Businesses

- Phishing
- Malware
- Ransomware
- Weak passwords
- Spoofed accounts
- Insider threats

Resist the myths: these misconceptions can wreck your cybersecurity posture

Many companies have dangerous blind spots when it comes to cybersecurity threats. As CEO, you set the tone for your business. If you understand the common misconceptions that prevent companies from properly protecting themselves, you can help shape the culture of your organization and avoid catastrophe.

| 1 | My business is too small to be attacked

Although SMBs have less valuable data than a large corporation, they're not safe from cyberattacks. Most businesses retain personal information like credit card numbers, protected health information and personally identifiable information, which can be used to perpetrate identity theft and other damaging scams.

|2 | Most hackers aren't dangerous

It's easy to think of a hacker as a bored teenager working from their parents' basement and looking to wreak havoc. While amateurs certainly exist, they are far outnumbered by specialized cybercriminals who operate like business owners – highly organized, disciplined and focused on a desired outcome. Cyberthreat actors are often well funded and able to enact highly sophisticated schemes and tactics quickly and ruthlessly.

| 3 | Firewall and antivirus software is the only protection I need

Antivirus software and a firewall are important components of any cybersecurity strategy. However, they have limitations. Today's threat actors can outsmart legacy technologies, making it impossible to detect a problem before it's too late. Additionally, CEOs need staffing to run 24/7 self-monitoring security protocols. It's a big mistake to over-rely on technology without having adequate staff in place to run it.

Cybersecurity & SMBs:

Quick Facts*

43% of cyberattacks target small business

60% of small businesses that are victims of a cyberattack go out of business within six months

47% of small businesses do not understand how to protect themselves against cyberattacks

3 out of 4 small businesses say they don't have the personnel to address IT security

54% of small businesses think they're too small for a cyberattack

25% of small businesses didn't realize cyberattacks would cost them money

83% of small businesses haven't put cash aside for dealing with a cyberattack

54% of small businesses don't have a plan in place for reacting to cyberattacks

*https://www.fundera.com/resources/small-business-cyber-security-statistics

| 4 | The authorities will save us if an attack occurs

Do not make the mistake of thinking that the authorities will come to save the day. Unfortunately, there are far too many cybersecurity incidents for law enforcement to pursue. If law enforcement is involved at all, the highest priority is likely given to the most severe attacks. Most SMBs are on their own when it comes to protecting their companies from and responding to cyberattacks.

|5 | It won't be hard to recover after an attack

The average cost of a cyberattack is more than $188,000 for small businesses (according to Symantec). However, that doesn't include the hidden costs: legal fees, lost productivity, losing the trust of your customers or worse, losing the entire business. There is no way of estimating the full damages if a cyberattack occurs.

Technology | People | Processes

SMBs may not have vast resources, but there are a number of ways CEOs can leverage solutions that combine technology, people and processes to build a solid cybersecurity framework.

Get the right technology

Antivirus software

Antivirus software is cost effective and defends against most types of malware. It's often the first line of detection to identify and stop a virus from wreaking havoc on IT systems.

Endpoint security solutions

Endpoints are the main doors that threat actors use to attack a business, including hardware, software and IT infrastructure. Endpoint security solutions cost about the same as antivirus software, and are often just as effective.

Firewalls

Firewalls help monitor internet traffic that flows to and from a network, blocking attempts from malicious websites and other dubious sources. Firewalls are an essential component of an effective cybersecurity plan, as they help protect a wide range of business operations.

Data backup

Having secure, reliable data backup in place is critical. With ransomware attacks at an all-time high, an effective data backup solution will allow you recover any information lost and minimize downtime.

Encryption software

If your business handles sensitive customer data, encryption software is a must. You'll want to protect employee records, customer information and financial records.

Multifactor authentication (MFA)

In today's threat landscape, MFA is a must-have. It is one of the best ways to secure your network, guard sensitive data and protect critical infrastructure – and it greatly reduces the likelihood of password cracking.

Train your people

Having the right technology is an important piece of a strong cybersecurity posture, but your technology must work in tandem with your people and processes. Make the most of your investments by:

Training your employees

Cybercriminals are betting on finding the weakest link in your security – and that's often your employees. According to the Ponemon Institute (via CSR), 54% of SMBs affected by data breaches stated that the root causes for the attacks were "negligent employees." Accordingly, end-user training is among the highest of priorities. In fact, training allows you to achieve the most results in the least amount of time.

Establishing a strong security awareness

Phishing is one of the most common forms of social engineering, and a lucrative one for hackers. Despite better training and awareness around this trend, cybercriminals have become quite good at tricking end users into trusting a malicious source. Make sure your cybersecurity plan includes phishing tests, and use it regularly to make sure your employees are remaining vigilant.

Performing regular testing

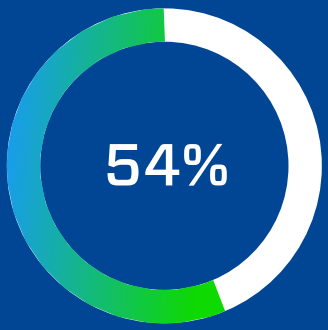
Testing helps ensure your cybersecurity systems are working as intended. The threat landscape becomes more sophisticated by the day, which means you'll want to maintain a regular schedule of testing to ensure that it protects against any emerging threats.

Verify your processes

The third component to a solid cybersecurity strategy revolves around robust policies, processes and procedures. At a minimum, you'll want to have policies that cover acceptable use, employee access to sensitive data, processes for routinely checking firewall and antivirus logs, and an incident response and recover plan spelled out far in advance of an actual breach. A consultant can be helpful in determining best practices that address unique concerns faced by SMBs.

Phishing was the most prevalent cyber threat in the US in 2020, with

241,342 victims.



54% of SMBs affected by data breaches cited "negligent employees" as the cause of attack

OTHER SOURCES

- Ponemon Institute, 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses, October 2019.
- CrowdStrike, 2020 Global Threat Report, 2020.

Do you know your company's security vulnerabilities?

A cyberattack could have occurred in the time it's taken you to read this guide. If it did, would you be prepared?

Our IT Risk Assessment is a quick, low-cost way to check your cybersecurity posture and thwart potential breaches. For $1,000, you'll receive a report analyzing:

- ✓ **Hardware**
- ✓ **Configuration**
- ✓ **Software**
- ✓ **Accessibility**

Protect your organization, your clients and your reputation by keeping your data secure.

TALK TO A CONSULTANT

Our Cybersecurity Services:

- ✓ IT risk assessment
- ✓ Vulnerability scanning and penetration testing
- ✓ Data breach response
- ✓ Incident response and disaster recovery plan creation/updates
- ✓ Virtual CISO
- ✓ Policy and procedure creation and updates