CAPCO

# CYBERSECURITY RISK MANAGEMENT FOR SMALL AND MEDIUM-SIZED BUSINESSES

CAPCO'S CYBERSECURITY INSIGHT SERIES

Cybersecurity threats for small-to-medium sized businesses (SMBs) are real. SMBs are just as likely as larger businesses to be attacked. Yet, many are much less prepared to detect and endure an attack. There is a path forward to significantly improve the risk posture of an organization with good cyber hygiene, a strategic roadmap, and a cybersecurity insurance policy.

# CYBERSECURITY CONSIDERATIONS FOR SMBS

Imagine this: It's tax season, and your HR director receives an email allegedly from the president asking to send copies of all your employees' W-2s. The HR director emails the files only to discover days later that the email came from a skilled hacker, who is using those W-2s to file fake tax returns.

These types of cybersecurity threats happen daily, which is why small-to-medium sized businesses (SMBs) are on high alert. Although many SMBs think the likelihood of a cyberattack is negligible because of their size or relatively low prominence in the media, these companies are, on occasion, even more likely to fall prey to a cyberattack. The unfortunate fact is **60% of small businesses close within six months of a cyberattack.**[1] With the cost of an attack varying between a few hundred thousand to over a million dollars, the financial, operational, and reputational costs of an attack are too much for a small or medium-sized business to withstand.

SMBs face a specific set of challenges and limiting factors when it comes to improving their cybersecurity posture. Their smaller size often makes it difficult to find cybersecurity champions and define a right-sized cybersecurity governance model. Most SMBs do not have a dedicated chief information security officer (CISO) or information security organization to champion cybersecurity efforts. In fact, 35% of SMBs have no one function that determines information security priorities, and 43% of SMBs have no cybersecurity defense plan in place.[2]

> *"60% of small businesses close within six months of a cyberattack."*

Small in-house and outsourced IT departments typically have limited expertise on cyber hygiene best practices and cybersecurity program management, and limited capacity for new projects or tools. These IT teams may also have initiatives underway to move infrastructure to the cloud and, with limited cloud security expertise, they are unknowingly opening the door to an entirely new arena for hackers to play in with their advanced cybercriminal tools.

[1] https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html
[2] https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report-Infographic.pdf

# 4 APPROACHES FOR IMPROVING YOUR CYBERSECURITY RISK POSTURE

Keep in mind that your approach to cybersecurity should be tailored to the size, industry, location, and type of operations specific to your organization, especially as it relates to newly adopted remote working models or investments in cloud-based technologies. To protect your SMB, follow these four steps to start building a cybersecurity strategy to withstand inevitable cyberattacks such as phishing, business email compromise (BEC), malware, and ransomware.

1. **Take stock of your current cybersecurity capabilities** and identify any gaps in baseline security requirements with a cybersecurity assessment. Industry standard framework, such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), is a quick and straightforward starting point.

2. **Conduct a cyber hygiene review** to first focus your cybersecurity programs on key fundamental requirements, before dedicating time and resources to more sophisticated technologies and tools that may not be the right fit to combat the most relevant risks. These baseline requirements should be implemented by all organizations regardless of size or industry to protect against the most common cyber threats using common sense solutions.

   **Start implementing these fundamental cyber hygiene practices:**

   - **Define and ratify a formal cybersecurity policy; if you process or store personal or sensitive information, develop a privacy policy for handling that data. Focus on:**
     - Password complexity and rotation
     - Multi-factor authentication
     - Data classification and encryption
     - Identity and access management
     - Remote access and work-from-home best practices
   - **Establish required training and awareness for all employees.** Top root causes of data breaches are often due to negligent employees or careless third-party partners.[3] [4] Focus on:
     - Strong password requirements and rotation
     - Phishing and BEC awareness
     - Appropriate use policies
     - Other cyber hygiene best practices (e.g., clean desk policy, data classification and protection, reporting mechanisms)
   - **Conduct and maintain an inventory of hardware, software, end user devices, and data that make up your organization.**
     - Assign criticality to these assets to prioritize recovery in the event of an attack
     - Leverage publicly available tools, such as the CIS Hardware and Software Asset tracker, if you need a starting place [5]
   - **Take regular backups of critical data and store backups either offsite or in the cloud.**
     - Test restoration of backups
     - Consider different scanning or health check solutions to ensure malware does not propagate to backups in the event of an attack

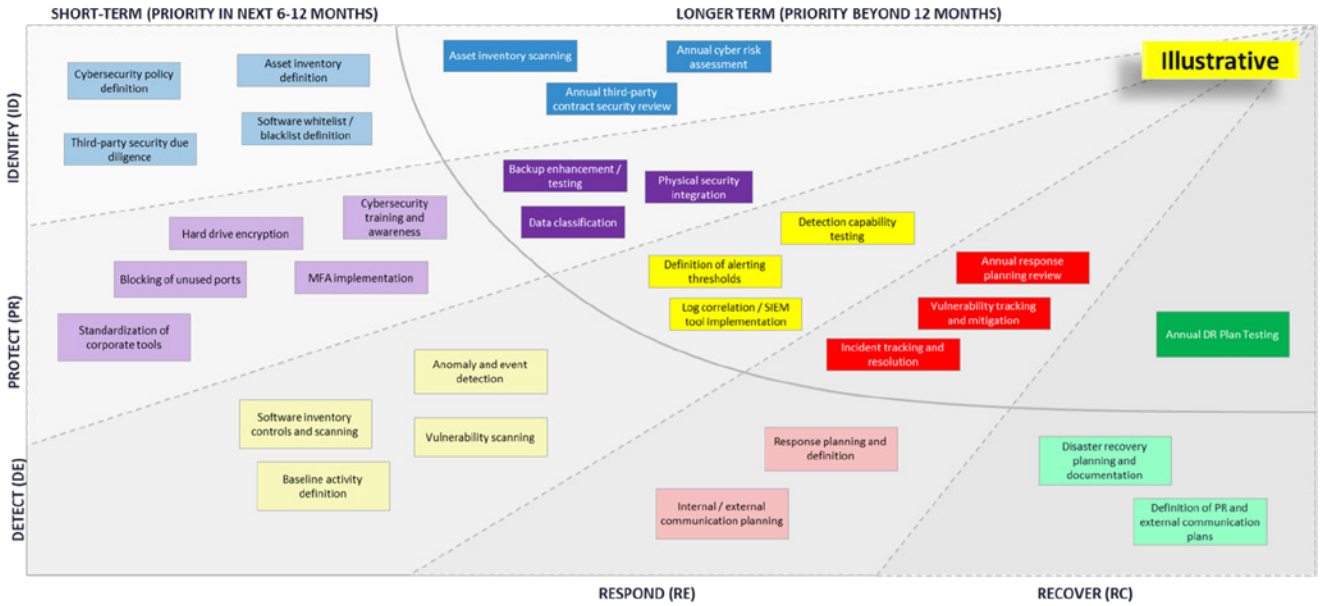
3. **Create a strategic roadmap.** Once a baseline of best practices has been reviewed and implemented, strategic and longer-term planning can be organized based on the current risk posture and risk appetite. Compose your roadmap with a series of project cards organized by NIST CSF function and prioritized for the short-term (6-12 months) and long-term (12-24 months).

[3] https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report-Infographic.pdf

[4] 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

[5] https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/

## ROADMAP WITH SHORT-TERM AND LONG-TERM PRIORITIES




Source: Illustrative roadmap based on Capco experience

**Short-term initiatives may include:**

- Define a **whitelist of approved software** (e.g., anti-virus software) and standardize corporate tools used across the organization (e.g., Dropbox, OneDrive)
- Define a **checklist for third-party security reviews** during the pre-contract phase of vendor negotiations (e.g., roles and responsibilities, data security)
- Document formal **recovery plans** for critical assets, including recovery time, service-level agreements (SLAs), processes and requirements

**Long-term initiatives may include:**

- Implement an **automated scanning solution** to reconcile and update asset inventory for network devices and installed software
- Implement a formal **data classification solution** for data and email to keep data privacy top of mind
- Implement a security information and event management **(SIEM) tool designed for SMBs** to aggregate and analyze data across platforms, identifying and mitigating threats before they cause damage

4. **Purchase a cybersecurity insurance policy.** This fast-growing sector of the insurance industry gives many SMBs peace of mind that they are covered when a cybersecurity incident occurs. Be aware that insurance carriers expect baseline security best practices and require a solid understanding of your cybersecurity policies and how you protect your assets to determine coverage details and premiums. The output of your cybersecurity assessment, as outlined in step one, can be used to purchase a cybersecurity insurance policy.

   Premiums can vary from a few hundred thousand dollars to $5 million, with the cost of based on:

   - Industry and type of non-public information (NPI) / personally identifiable information (PII) stored
   - Who has access to your systems and data
   - Network security requirements and policies
   - Your claims history of past cybersecurity incidents[6]

[6] https://www.progressivecommercial.com/business-insurance/cyber-insurance/cyber-insurance-cost/

**Case Study: Cybersecurity Assessment for a European Investment Fund**

A European investment fund sought a partner to perform a review of the office's cybersecurity capabilities. The objective of the assessment was to determine the client's cybersecurity posture in collaboration with IT, legal, and business stakeholders, in the absence of a dedicated security role. In parallel, the organization was looking to validate its internal team's awareness and readiness to respond to future cybersecurity incidents through a facilitated tabletop simulation exercise. Capco leveraged its past experience in assessing cybersecurity capabilities of both large and small financial services institutions and tailored its proprietary approach to meet the needs of this particular organization.

The output from this assessment was used to communicate to our client's cybersecurity insurance carrier and to consolidate a list of cyber hygiene recommendations and longer-term strategic initiatives. These deliverables enhanced the firm's cybersecurity awareness, illustrated the current understanding of cybersecurity roles and responsibilities across teams, and provided a maturity benchmark against which to measure future progress.

**Conclusion: The Best Defense Is a Good Offense**

Make it a priority to protect your data for the benefit of your employees and customers and the long-term health of your business. Hackers have no prejudice. These criminals will invade your organization, regardless of its size, prominence, or location, with their sophisticated tools. SMBs are under attack as never before, a trend the pandemic has only accelerated with newly adopted remote work.

It's no longer an option for SMBs to simply adopt a defensive plan to ward off an anticipated attack. SMBs need to go on the offense by taking stock of their current cybersecurity capabilities, conducting a cyber hygiene review, creating a strategic road map, and investing in a cybersecurity insurance policy.

One door left unlocked is enough to result in significant financial losses, many unhappy customers, and headlines that no CEO or investor wants to read.

## AUTHORS

**Julien Bonnay**, Partner, julien.bonnay@capco.com
**Jayadevan Vijayakrishnan**, Managing Principal, jayadevan.vijayakrishnan@capco.com
**Alex Donovan**, Senior Consultant, alex.donovan@capco.com

## ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

## WORLDWIDE OFFICES

### APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

### EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

### NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

### SOUTH AMERICA
São Paulo

**WWW.CAPCO.COM**

CAPCO