# Cybersecurity for the C-Suite

## A GUIDE TO MANAGING CYBERSECURITY RISK FOR BOARD MEMBERS AND EXECUTIVES

Digital transformation, the integration of digital technologies into all aspects of an enterprise's operations, has made cybersecurity more important than ever. Digital transformation has enabled numerous benefits including improved customer experience, data-driven decision making, and faster innovation and time-to-market. Digital transformation has also resulted in targets for malicious actors who have increased efforts to hack enterprises for financial or other gain. In response to these malicious actors, enterprise technology companies have increased investment in cybersecurity activities, and governments have enacted laws and policies that introduce requirements for companies.

> *Cybersecurity—the practice of protecting the confidentiality, integrity, and availability of information and information systems from threats and vulnerabilities.*

An overwhelming majority of companies across all sectors rely on information technology (IT) to operate critical business processes. Increasingly, this IT includes embedded artificial intelligence. Companies expect these products both to function well and provide appropriate security, an issue about which customers increasingly ask their third-party service providers.

Disruptions to a company's IT systems reduce revenue, damage brands, and even result in fines and other legal consequences. Some of a company's legal requirements are proactive (e.g., disclosing the role their board of directors plays in managing the enterprise's cybersecurity risks) while others are reactive (e.g., reporting certain cyber incidents).

Within this context, it is clear that cybersecurity responsibilities are not limited to a CIO, CISO, or IT team, but that if your company is going to continue to enjoy the benefits of digital transformation and meet your legal obligations, then you must manage your company's cybersecurity risk effectively. Indeed, having a plan to respond to and recover from a cyber incident, along with a dedicated team of incident responders and cybersecurity experts on standby can prepare your company to not just bounce back, but leap forward.

As a board member or executive, you do not need to be a cybersecurity expert. Your company's security team will determine if there is an exploitable vulnerability. However, to optimize your cybersecurity resources, your company's security team will need your expertise to determine how to value your company's assets and the likely impact of a potential cyber incident to your company's health or bottom line.

*Artificial Intelligence—software designed to use data to perform functions historically associated with human intelligence, such as reasoning, learning, decision making, and self-improvement.*

## Foundations of Cybersecurity Leadership

To effectively manage cybersecurity risk, a board member or executive needs to understand three foundational truths about cybersecurity:

- **Leadership influences cybersecurity.** From establishing culture and accountability, allocating resources, setting internal policies, supporting education and training, working with suppliers, and investing in technology, how you approach cybersecurity will reverberate throughout your company.
- **Cybersecurity is a strategic business issue.** Done well, good cybersecurity risk management can be a way your business differentiates itself from competitors.
- **Cybersecurity is all about risk management.** As an executive, you know how to avoid, mitigate, transfer, or accept risk, and your company should integrate cybersecurity risk management into its broader risk management activities.

BUILDING ON THESE FOUNDATIONAL TRUTHS, YOU SHOULD

1 Understand Your Company and Its Operating Environment

2 Appreciate Cybersecurity at the Strategic and Operational Levels

3 Navigate Building an Effective Cybersecurity Strategy

**Ultimately, these actions will prepare you to leverage cybersecurity to deliver value.**

## 1 Understand Your Company and Its Operating Environment

Your company's operating environment is the context in which risks emerge, and understanding it is critical for you to make effective decisions.

### Internal Context

- **IT infrastructure,** including your company's attack surface and challenges created by legacy software
- **Human capital and culture,** including your company's recruitment, training, and retention plans
- **Budget and other resources,** including the long-term benefits of investing in cybersecurity today

### External Context

- **Threat landscape,** including geopolitical, sector-wide, and company-specific threats
- **Legal requirements,** including both general and sector-specific laws
- **Third-party dependencies and supply chain risk,** as well as third-party cybersecurity partners

## 2 Appreciate Cybersecurity at the Strategic and Operational Levels

Your strategic-level decisions support five operational-level activities. While these operational activities may not be your direct responsibility, understanding and appreciating these activities will better prepare you to make strategic decisions and support the teams responsible for cybersecurity operations.

- **Identify.** Catalogue your company's assets to understand what you need to protect.
- **Protect.** Select and implement security controls to safeguard your company's information and information systems.
- **Detect.** Develop or obtain through third-party service providers capabilities to discover malicious activity, including measuring and investing in technologies to improve Mean Time to Detect (MTTD).
- **Respond.** Formalize a cyber-incident response plan and exercise it regularly to prepare to minimize impact and return to normal operations, including measuring and investing in technologies to improve Mean Time to Respond (MTTR); execute the plan if necessary.
- **Recover.** Restore full functionality and improve your company's ability to identify, protect, detect, respond to, and recover from malicious activity.

## 3 Navigate Building an Effective Cybersecurity Strategy

There is no checklist for a good cybersecurity strategy. Cybersecurity is too complex for such an approach. Your company's operational environment is constantly changing, malicious actors are continuously adapting, and the services enterprise technology companies provide are constantly improving. As a result, a traditional road map that shows a well-defined path from point A to point B is ineffective. Rather, a board member or executive needs a compass, a tool that continuously adjusts but always points toward your desired destination. In other words, like other issues you manage, rather than sticking to a predetermined plan, cybersecurity requires maintaining a sense of direction, adjusting to changing conditions, learning from experience, and being agile.

**USING YOUR COMPASS, YOU SHOULD OVERSEE, LEAD, OR PARTICIPATE IN THESE FOUR ACTIVITIES.**

### Set a Vision

Account for your company's risk tolerance and appetite.

. . . . .

Define your company's priorities and target cybersecurity profile.

### Build a Structure

Select a framework to guide your cybersecurity risk management activities.

. . . . .

Define roles and responsibilities.

. . . . .

Recruit and retain the right people.

### Allocate Resources

Differentiate your company's assets based on importance to your mission.

. . . . .

Align your company's budget with your company's cybersecurity priorities and target profile.

### Oversee Execution

Develop key performance indicators.

. . . . .

Test your capacity.

. . . . .

Hold your team accountable.

# Delivering Value Through Effective Cybersecurity Risk Management

Digital transformation has elevated the significance of cybersecurity, extending the responsibility of effective cybersecurity risk management beyond IT teams, and to boards and executives. One reason cybersecurity risk management is part of the domain of executives is that it is too complex for one-size-fits-all approaches. A company needs to develop a vision, build an organizational structure, allocate resources, and oversee execution. Ultimately, these activities will help a company differentiate itself from its competitors and deliver value to its customers and community.