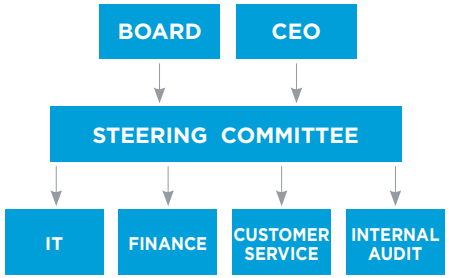
CYBER RISK MANAGEMENT PROGRAM

CENDROWSKI CORPORATE ADVISORS
a different perspective™

This guide is designed to help an organization understand the many functions that should be considered in a comprehensive cyber risk management program. The guide may be used as a benchmark to diagnose your current readiness, or as a roadmap to improve or implement your plan. However, consulting with a business advisor specializing in cyber risk management is critical to help ensure your organization is adequately protected.

Cybersecurity, like any other risk management program, is a cultural initiative. Each member of the organization needs to understand their role in cyber risk management, and be aware of potential intrusion attempts and warning signs of intrusion. For example, even non-technical users should be aware of the dangers of a strange email asking for login credentials or a device that starts behaving differently.

Cybersecurity is also a cross-functional initiative – it is not solely an IT issue, although IT certainly has a prominent role in the process. The cyber risk management program should be organized and driven by a cross-functional team with the highest corporate sponsorship. In many organizations, it would be appropriate for Cyber to be a board-level subject, with the sponsorship and support of the CEO.



NOT A STATIC ISSUE OR SOLUTION: The risk environment is extremely chaotic and new threats are continuously emerging. The cyber risk management program will identify new risks and threats that will need to be rapidly assessed and remediated. The organization must therefore develop nimbleness to be able to rapidly react and adapt to an environment of rapidly evolving threats, and resiliency to rapidly respond to detected intrusion. The need for organizational nimbleness and resiliency is what drives the need for a cross-functional team.

The cyber risk management process includes five functions to address risk:

- **Identify** – Catalog critical data, systems, and hardware.
- **Protect** – Assess security and upgrade/replace weak assets, manage physical security.
- **Detect** – Monitor internal and external environments for emerging threats and signs of intrusion.
- **Respond** – Rapidly prevent escalation of an intrusion and identify root cause. Eliminate intrusion vector and repair damage.
- **Recover** – Manage public relations, customer notification and reporting.

These functions are expanded into sub-processes in the model on the reverse of this guide. Each of these subjects should be considered in the context of your environment and risk profile. To implement a comprehensive cyber risk management program, an organization should consider each of these functions and scale the response to reflect the overall risk profile of the organization.

Finally, the cyber risk management program is not a one-time exercise. Your risk model and processes to identify, protect, detect, respond, and recover must be ongoing and constantly managed to identify and address emerging risks. The actions and activities in your program must be built into everyone's daily activities and thought processes throughout the organization.

RISK PROFILE:

The organization should consider their overall risk profile related to cyber risk. Consider the impact to the organization if a cyber-intrusion were to occur. The questions below can help determine some of the major drivers of impact:

- Is your company part of critical infrastructure?
- To what extent would your customers or trading partners be affected by an outage at your company?
- What kinds of sensitive information (e.g. intellectual property, classified information, customer personal information) does your organization maintain?
- What customers would need to be notified if your organization had a security breach?

CYBER RISK MANAGEMENT PROCESS

CYBERSECURITY *IS* RISK MANAGEMENT℠

IDENTIFY

- Catalogue the critical data you have in your organization. Consider the business impact if it were released or damaged
- Catalogue the internal and external systems utilized by your organization
- Understand relationships, dependencies, shared data with key customers/ suppliers
- Establish/align organizational roles and responsibilities for security
- Identify legal/regulatory risks including contractual obligations
- Risk assessment of vulnerabilities & threats. Prioritize risks based on potential impact/likelihood

PROTECT

- Manage access to systems, including physical, remote, and user authorities
- Ensure all users & stakeholders understand their role in cyber protection; provide training regarding risks
- Identify legal and regulatory security requirements
- Ensure cybersecurity addressed in governance and risk management programs
- Implement sound information protection policies and procedures, including change controls, backups, and recovery programs
- Perform adequate maintenance; implement protective technology where appropriate

DETECT

- Identify baseline of operations; monitor for unexpected access, events, messages
- Monitor network, physical environment, personnel activities for unauthorized actions
- Detect unauthorized programs, malicious code; monitor system logs
- Perform vulnerability scans
- Define roles and responsibilities for detection processes and communications chain

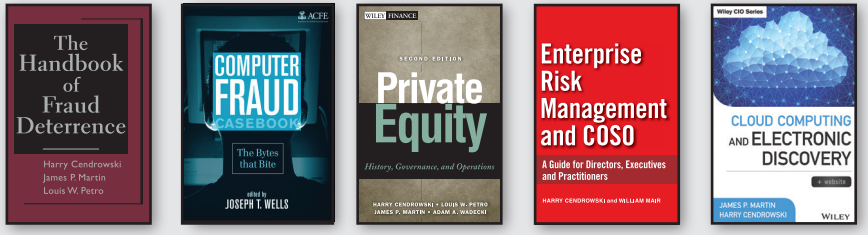
RESPOND

- Proactively develop and test response plans including identification of external advisors
- Consult with counsel regarding event and business impacts
- Understand business impact of the incident
- Identify root cause of the incident
- Contain incident and mitigate damage
- Update response plans and strategies based on incident

RECOVER

- Manage public relations/ repair reputation
- Update recovery strategies based on evolving best practices
- Manage legal issues

VOLUMES OF DOCUMENTED EXPERTISE BY MEMBERS OF THE CCA TEAM



The Business of
LINKING OPERATIONAL INTEGRITY
For more than 30 years

CHICAGO / BLOOMFIELD HILLS / 866-717-1607 / CCA-ADVISORS.COM