CMMI Institute
AN ISACA ENTERPRISE

Getting Your Board to Lean into Cybersecurity

Developing a common understanding of enterprise cybersecurity readiness, resilience and risk may help ease your board-level concerns.

Every year brings board members more compelling reasons to care about the importance of establishing enterprise cybersecurity programs to help prevent lawsuits, regulatory fines, loss of public reputation, hits to share prices, damaged careers and other terrible costs of data breaches.

Yet, boards of directors seem uncertain about the efficacy of their organization's cybersecurity efforts and unclear about the best ways to fulfill their own growing oversight responsibilities in this increasingly crucial risk management area. Consider the results of two major surveys:

- 58 percent of board member respondents at public companies surveyed by The National Association of Corporate Directors (NACD) named cyber-related issues as the most challenging risk they are expected to oversee. [1]

- Cybersecurity policies and defenses were the number one corporate governance technology challenge cited in an ISACA global study. Some 53 percent of organizations polled said malicious attacks were rising, but 48 percent lacked confidence in their organization's ability to respond to complex threats. [2]

Culprits: Lack of Information and Knowledge

What's behind these poor perceptions of protection? Why does cybersecurity oversight remain a big challenge for directors? A lack of knowledge coupled with underdeveloped strategy lies at the root of these governance problems.

"Boards struggle today with how to provide oversight for cybersecurity because they don't feel like experts," says Pete Chronis, Chief Information Security Officer at Time Warner's Turner division, in a recent *Wall Street Journal* article. "Members don't need to be experts themselves," he says, just interested and "enlightened" enough to ask senior

IT leaders fundamental questions about assessing, addressing and prioritizing risk, in the context of business goals. [3]

Gaining that enlightenment appears to be a widespread problem. The ISACA study found only 21 percent of organizational leaders are briefed on risk topics at every senior team meeting. In the NACD survey, 22 percent of directors expressed dissatisfaction with the *quality* of cyber-risk information provided by management. Most criticized: Information that doesn't provide enough transparency into problems (44 percent) or doesn't allow effective external or internal benchmarking (41 percent).

Get With the Program

It's clear that senior security leaders must do a better job establishing and communicating with board members about stronger, more mature enterprise programs. Doing so will require more actively informed and engaged board members to confidently fund, support and guide new efforts to guard the organization's "crown jewels." What's the best way to go?

The CMMI Cybermaturity Platform from the CMMI Institute gives senior leaders a systematic way to work together on creating enterprise security management strategies and protections. Introduced in April, the program helps organizations climb the cybersecurity maturity ladder — from a "check-the-boxes," compliance-driven, project-based mindset to a new understanding of security as a key business strategy.

The program guides creation of a comprehensive cyber-protection architecture that includes a governance framework, which helps executives to identify and manage risks while ensuring effective mitigation, detection and response. The key: developing a common understanding of enterprise cybersecurity readiness, resilience, and risk and then, scaling capabilities appropriate to the challenges. This approach lets leadership teams frame the business case, prioritize resources and investments, and provides a way to benchmark progress.

How It Works

The CISO or CSO starts by defining the scope of assessment, risk profile, and maturity targets. Working with Operations, their teams assess four key enterprise security areas: threats, risk-based targets, gaps and industry comparisons. Focus is on three key areas: SecOps, Capability Maturity, and Workforce Readiness.

Using available data, each potential vulnerability is assigned a likelihood and impact ranging from very low to very high. Based on these inputs, the CISO develops a risk-mitigation roadmap for board prioritization and approval. Recommendations and results are presented to directors in simple graphics and lay terms and use the familiar lens of people, process and technology.

Payoffs

The CMMI approach yields several benefits: Enterprises can more easily set practices and capabilities. Boards are better informed so they make wiser decisions. Organizations see where they stand on a five-stage maturity scale and how they perform against industry benchmarks. A dynamic framework encompasses leading standards and controls (*ISO, NIST, COBIT, DHS, ISC2)* and helps executives keep up with new threats, technologies and best practices.

Most importantly, enterprises can confidently answer key questions:
"Is our level of investment right?"
"Are we addressing the most important issues?"
"What are our competitors doing?"
"What framework or standard do we choose?"

A Framework for Partnership

Today's boards want and need a more active role in ensuring effective cybersecurity. By aligning pragmatic insights on security risks with strategic objectives, CISOs, CSOs and other high-level IT leaders have an unprecedented opportunity to build both stronger partnerships and protections.

#

Sources

1. "National Association of Corporate Directors 2017-2018 Public Company Governance Survey" https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=50360

2. "Better Tech Governance is Better for Business", ISACA Survey Report, 2017

3. https://www.wsj.com/articles/the-corporate-boards-role-when-it-comes-to-cybersecurity-1513652940