Risk Oversight

Facing Cyber Threats: Keys to Security, Vigilance, And Resilience

By Mary E. Galligan

The financial, operational, legal, security, and reputational risks posed by cyber threats are serious, and no organization is immune. Oversight of these threats and of their management falls squarely within directors' governance responsibilities. With virtually all large public companies facing myriad cyber threats, how can board members best conduct that oversight?

The answer is: "It depends"—on the company's industry, operating model, risk management program, risk tolerance, information technology (IT), data, and vulnerabilities. Oversight, however, starts with the board's understanding of potential cyber threats and what management is and should be doing in response. A bit of background and a few guidelines can help boards hold productive discussions with management regarding this critical area.

Who is posing what threats? Cyber threats arise from the activities of three broad types of actors:

- "Hacktivists" usually aim to disrupt websites or IT-based operations, often to generate denial-of-service situations and information theft. Like "activists," they may be protesting organizational policies, although disgruntled former (or current) employees may also fall into this category.
- Cyber criminals pursue data theft for profit, and may act as independent contractors to other criminals. They drain bank accounts; steal the private data of customers, executives, or directors; or lightly skim repetitive, high-volume electronic transactions to divert funds to their own accounts, among other crimes.
- Perpetrators of corporate espionage generally target trade secrets and intellectual property, as well as strategic plans, deal memos, customer lists, and internal communications.

Combating cyber threats extends beyond the purview of the chief information officer (CIO) and chief security officer (CSO). These key individuals need the support of the CEO in leading the threat-management effort, together with the chief operating officer, chief financial officer, chief legal officer, and other senior executives, while the board exercises oversight. That said, the CIO or the CSO, or both, can usually answer the board's initial questions.

Where to begin? The board, the board risk committee (if present), or a subset of the board can start by reassuring the CIO and CSO that their functions will not have to drop everything in order to react to piecemeal concerns. Guarding against cyber threats should be a mind-set across the entire organization, devoted to achieving security, vigilance, and resilience.

- *Security* of data and systems centers on risk-prioritized policies, procedures, and controls, such as those for devices, e-mail, home-based data, and third-party data use (the latter now common in many vendor and outsourcing arrangements).
- *Vigilance* means rapidly flagging violations and suspicious occurrences, and responding appropriately. It also includes being adaptive—absorbing new threat information and adjusting to changes in the business and technology environment to keep eyes on what matters most.
- *Resilience* centers on post-attack recovery, which should be swift and aimed at damage control and repair. As a first step to gauge vulnerabilities, directors might ask:
  - How do we determine what information is leaving the organization, and how?
  - What are the greatest cyber threats our organization faces?
  - What are the "crown jewels" that we must protect?
  - Which other data require strong protection?

The answers will help the CIO and CSO consider specifics. They also set the tone for transparency and a two-way conversation, and set up a "ladder" approach in which threats are arrayed by risk and managed with the appropriate priority and resources.

Effective approaches to the oversight of cyber threats resemble other effective risk governance efforts. They rest upon collaborative conversations with management, sound policies and procedures, constant monitoring, regular reports and reviews, solid response planning, and the ongoing education of the board.

Mary E. Galligan is a director in the Security & Privacy practice of Deloitte & Touche LLP, following her recent retirement from the Federal Bureau of Investigation.