Cyber Risk

Sharpening the Board's Role in Cyber-Risk Oversight

By Deborah DeHaas and Ed Powers

Cyber risk has become one of the top enterprise-wide risks facing companies. From a governance perspective, one of the board's most important tasks is to verify that management has a clear perspective of how the business could be most seriously impacted, and that management has the appropriate skills, resources, and approach in place to minimize the likelihood of a cyber incident—and the ability to mitigate any damages that could occur.

Boards can take various approaches to fulfill their cyber-risk oversight duties. For example, some boards have a separate entry on their risk map to monitor cyber risk and make it a full board responsibility. Others keep oversight within the domain of the audit or risk committee. Whichever applies, cyber risk should be on board or committee agendas annually, if not more frequently.

Management's duty is to align the cyber risk program to a detailed business risk profile. This profile should reflect an understanding of likely attackers, their objectives, which assets are most at risk, and the impact of those assets being compromised. When alignment is off, it's the board's duty to challenge management to construct a more tightly aligned program. In their oversight role, boards need to know the right questions to ask and how to monitor the effectiveness of management's plans and responses. Such questions may include: Who is the appropriate executive to be leading cyber risk management? What are the greatest cyber threats our organization faces? What are the "crown jewels" that we must protect, including data and other assets?

The following are other issues for boards to consider when developing processes for cyber-risk oversight:

Assessing cyber program costs. Cyber incidents have both hard costs (e.g., fines, public relations costs, drops in shareholder value) and soft costs (e.g., losing customers, reputational damage) that need to be weighed. An understanding of the potential financial impact of an attack can help organizations calibrate their levels of investment. Boards should understand management's rationale for investing and allocating resources to monitor cyber risk, guard against it, and expedite response and recovery. Among the questions boards can ask are: How will spending allow the organization to see and anticipate threats, and to quickly recognize when an attack has occurred? How will management's plan support the organization's ability to restore confidence after an attack and minimize the business impact? Is cyber insurance appropriate, and if so, what type and level of coverage are needed, and at what cost?

Developing board-level metrics and benchmarking. Boards need useful metrics and analytics to gauge whether the organization is managing cyber risk at an acceptable level. Management can work with directors to develop a dashboard to identify the parts of the business with the greatest and least amounts of cyber exposure and the initiatives in place to mitigate risks. Boards can also ask management about its use of risk-sensing tools. A recent global survey of C-level executives conducted on behalf of Deloitte Touche Tohmatsu Ltd. found that while many organizations have risk-sensing capabilities, they often overlook key elements and lack technical depth.

Participating in war-gaming exercises. Cyberattack simulations and other war-gaming exercises can help identify vulnerabilities and gaps in preparedness and improve the ability of management teams to make decisions under stress. Leading organizations involve management directly in such exercises; for some, it might make sense to include relevant board members as well.

Determining the voice of the organization during a cyber incident. In a crisis, a quick response is essential. Management is often the first voice of the organization; however, crisis plans should consider the board's role and where it might be appropriate for the board to be a voice in the dialogue with stakeholders, particularly shareholders.

As the board's role in cyber-risk oversight evolves, the importance of having strong, dialogue with management cannot be overestimated. Without close communication between boards and management, the organization could be at even greater risk.

Deborah DeHaas is vice chair; national managing partner, Center for Corporate Governance; and chief inclusion officer at Deloitte LLP. Ed Powers is national managing principal, Cyber Risk Services, Deloitte & Touche LLP.