Board Directors Need to Have Discussions on Which Risks to Avoid, Which Risks to Accept, and Which to Mitigate Through Insurance

Total cybersecurity is an unrealistic goal. Cybersecurity is a continuum requiring strategic decision-making about where and how to spend security dollars.

Attempting to guard every system equally is a recipe for exhausting the budget on low-priority systems. And it'll result in bad security, since the company's crown jewels will lack the sophisticated protections they need.

In 2014, and again with a revised edition in 2017, the National Association of Corporate Directors teamed with the Internet Security Alliance to produce a handbook guiding directors in overseeing this difficult terrain.

On June 21, NACD, in partnership with ISA, hosted a full day event in Chicago that brought together directors, executives, and cybersecurity experts to share real-world insights and critical action steps for boards to foster enterprise-wide cyber resiliency.

Among the five principles that NACD suggests directors consider as they oversee the board's work is to discuss which risks to avoid, which to accept, and which to mitigate or transfer through insurance. Directors should develop specific plans associated with each approach.

Adopting a risk-based attitude toward cybersecurity can be easier said than done. A recent AFECA study (pdf) found companies typically want to apply security measures equally to all data and functions. Until recently, technologists reinforced this way of thinking by discussing cybersecurity in terms of digital moats and walls to keep bad actors out.

Today, we know that even strong walls have cracks wide enough for hackers to slip through. Systems whose penetration or disruption would cause major damage need multi-layered protection, and it's okay to pay for security on low-risk systems only to the level that their impact justifies.

As boards exercise their oversight, here are a few things they should consider:

- What data, and how much data, is the company willing to lose or have compromised?

Risk management means determining what level of cyber risk the company is willing to accept as a practical business consideration. Directors should know enough to distinguish between mission-critical assets and other data that is important, but less essential.

- How should cyber-risk mitigation investments be allocated among basic and advanced defenses?

Boards should encourage management to frame cybersecurity spending in terms of return on investment, and to reassess ROI regularly as the costs of protection, asset priorities and the nature of the threat all change over time.

- What options are available to assist in mitigating cyber risks?

Organizations of all industries and sizes have access to end-to-end solutions that can lessen some portions of cyber risk. They include preventative measures, governance measures, employee training, incident responses services and consulting. The nature of these services again demonstrates the importance of moving cybersecurity outside of the IT department into the context of enterprise-wide risk and strategy. This is a running theme of the handbook.

- What options are available to consider to assist in transferring certain kinds of cyber risks?

Cyber insurance can provide reimbursement for unexpected financial losses related to cybersecurity incidents such as data breaches or denial-of-service attacks. It's important to choose a carrier with the breadth of capabilities, expertise, market experience and capacity for innovation that best fits the organization's needs.

- How should the company assess the impact of cybersecurity attacks?

Conducting an assessment can be challenging, since there's a number of variable factors involved. For example, public or regulatory perception over company reaction to a data breach can drastically alter the risk calculus. Reputational damage and associated impact may not correspond directly to the size or severity of the event. Boards should seek assurance from management that it has carefully thought through these implications in devising organization priorities for risk management.

Written by David Perera, ISA Assistant Vice-President for Government and Policy