Boards Need Access to Adequate Cybersecurity Expertise – And Need to Give it Adequate Time on Meeting Agendas

Cyber literacy can be considered similar to financial literacy – not everyone on the board is an auditor, but everyone should be able to read a financial statement and understand the financial language of business.

As we all know, cybersecurity is very much a moving target. The threats and vulnerabilities change almost daily, and the standards for how to manage and oversee cyber risk are only beginning to take shape.

As the cyber threat grows, so too does the responsibility and expectations of board members. Directors need to do more than just simply understanding that threats to their organization exist. They need to be able to approach cybersecurity risk management the same way they approach discussions about strategy and company performance. To do this, boards of directors need access to adequate cybersecurity expertise.

This is not to say every board must add a cybersecurity and/or IT security expert to their board. Some organizations may decide this is right for their organization, others may not – there is no one-size-fits-all approach. Besides, with the severe shortage of senior-level cybersecurity talent, adding a cyber expert to every board isn't really realistic.

What is critical, however, is the need for boards to have access to adequate cybersecurity expertise. There are several ways directors can take advantage of to bring knowledgeable perspectives on cybersecurity matters into board room discussions, such as:

- Scheduling deep-dive briefings or examinations from independent and objective third-party experts validating whether the cybersecurity program is meeting its objectives
- Leveraging the board's existing independent advisors, such as external auditors and outside counsel, who will have a multiclient and industry-wide perspective on cyber-risk trends
- Participating in relevant director-education programs, such as NACD's Cyber-Risk Oversight program, which is modeled after the Cyber-Risk Oversight Handbook created by NACD and ISA.

Many boards are even incorporating a "report-back" item on meeting agendas to allow directors to share takeaways from outside educational and training programs with fellow board members. Doing so helps boards communicate cybersecurity issues to each other in a strategic, business-oriented way that increases overall board awareness of security issues.

Boards must also give cyber-risk management regular and adequate time on board meeting agendas. Unfortunately, in 2012, fewer than 40 percent of boards regularly received reports on privacy and security risks, with some boards never receiving such information.

Luckily, since then, we have seen a cultural shift, with more than 90 percent of public-company directors saying their boards discuss cybersecurity issues regularly and receive regular updates from management teams. But, the quality of the information provided during updates is lacking.

When asked to assess the quality of the information provided by senior management, nearly a quarter of directors were dissatisfied.

Why such high levels of dissatisfaction?

Boards are having difficulty using and interpreting the information to benchmark performance, both internally and externally, and there's insufficient transparency about performance as management teams tend to downplay the true state of the risk environment as well. Metrics to quantify the business impact of cyber threats and associated risk-management efforts are often lacking within organizations.

Cybersecurity and cyber-risk analysis are relatively new disciplines and it will take some time for reporting practices to mature. It is the responsibility of boards to ask the hard, uncomfortable questions of their senior management and give cyber-risk management regular and adequate time on board meeting agendas to discuss those questions.

There are resources and guidance available to help boards navigate this new digital environment. The Cyber-Risk Oversight Handbook, which NACD published in collaboration with ISA and AIG, provides a handy guide that can assist boards in addressing issues, such as the appropriate metrics to use in assessing management's cybersecurity processes and what questions to ask in the event of a breach.

Board members must set clear expectations with management about the format, frequency, and level of detail of the cybersecurity-related information they wish to receive. Because cybersecurity is more than just an IT issue, the board must bring its judgment to bear and provide effective guidance to management.

Cybersecurity needs to be woven into an organization's key systems and processes from end to end – and it starts with directors' understanding that their oversight of risk management includes cybersecurity issues and must be addressed during board meetings. Boards must ensure their company's cybersecurity strategy is appropriately designed and sufficiently resilient given its strategic imperatives and the realities of the business ecosystem in which it operates.

Written by Larry Clinton, ISA President & CEO, and Stacey Barrack, ISA Senior Director