Directors Discuss the Challenges of Cyber-Risk Oversight

March 2, 2018

By Jim De Loach

Companies today fall into two groups: those that have been breached and know it, and those that have been breached but *don't* know it. The realities of managing cyber risks are that breach risks are impossible to eliminate, resources for managing them are finite, risk profiles are ever-changing, and getting close to secure is elusive.

Our December 2017 discussion with a group of active directors during a dinner roundtable at a National Association of Corporate Directors (NACD) event identified some interesting insights into cyber-risk oversight at the board level.

Winning battles does not necessarily win the war. The discussion focused on how state-sponsored attacks targeting government institutions, industrial facilities, infrastructure, and many business organizations are increasing in both power and sophistication. Combatting so-called advanced persistent threats (APTs) requires faster detection and more advanced response tactics. In the arms race to keep pace (or, in most cases, catch up) with these threats, organizations need to commit adequate resources to tapping into available government intelligence and using it to facilitate their preparedness. Directors should suggest to their management team that they develop and maintain relationships with the correct contacts in the government sector needed to stay informed of emerging risks.

Upgrading detection capabilities. If management and the board believe the entity is an APT target based on what it represents, what it does, and the intellectual property it owns, the directors raised concerns over the maturity of most companies' cybersecurity countermeasures and what can be done from the board level to encourage more effective mitigation of the risks. Capabilities need to be upgraded beyond the controls, tools, and response mechanisms traditionally used to contain sophisticated attackers and corporate insiders. Our experience is that detective and monitoring controls remain immature across most industries relative to the evolving threat landscape.

Clarifying expectations with management. One director noted that when a chief information officer (CIO) or chief information security officer (CISO) asserts, "Don't worry, we're taking care of that," or delivers a similar pushback, it tends to stifle the dialogue and leaves directors with nowhere to go and an incomplete understanding of cyber-risk mitigation. The group's ensuing discussion pointed to several themes. Directors should ask the right questions (an appendix in the 2017 NACD publication on cyber risk oversight suggests relevant questions), consider changing board composition if more expertise is necessary, and establishing a separate cybersecurity or technology committee of the board. Although directors have limited time to get into details, they should set clear expectations for management at all levels with respect to cyber incidents that can affect the company's reputation, brand image, and standing with customers. Expectations regarding cybersecurity strategy and risk tolerances should be incorporated into the entity's risk appetite statement.

Directors Discuss the Challenges of Cyber-Risk Oversight

Continued

Improving board cybersecurity reporting and metrics. The severity of the Equifax breach as well as others raises the question as to whether boards are probing deeply enough to determine what they don't know. To that end, the directors noted that too often board reports deliver high-level information only. So, the question then becomes, what reporting and metrics on cybersecurity should the board request? The discussion pointed to several examples of key areas to consider:

The number of system vulnerabilities

- The length of time required to implement patches
- The length of time to detect a breach
- The length of time to respond to a breach
- The length of time to remediate audit findings
- Percent of breaches perpetrated through third parties
- The number of security protocol violations

Paying attention to "blocking and tackling." The group brought up several cybersecu-rity issues, including prioritizing high-risk patches, raising awareness of phishing, implementing security segmentation, and refreshing incident response and recovery plans continuously. One director noted that every organization should have multi-factor authentication access controls in place; accordingly, the board should discuss this security measure with management.

Conducting independent cybersecurity assessments. As innovative transformation initiatives constantly expand an organization's digital footprint, they outpace security protections companies have in place. Accordingly, organizations should consider assessing the current state of their overall cybersecurity using an established framework, in relation to their desired state. If such reviews identify gaps or areas of weakness requiring immediate remediation, the board should satisfy itself that management addresses those areas in a timely manner.

Being aware of challenges in the information technology (IT) and security organizations. The point was raised that many organizations need to seriously consider re-architecting themselves from both a technology and security standpoint. The question the board needs to ask management is: How quickly are we able to get an issue resolved? Management assertions that a solution will disrupt existing operations and legacy systems and, thus, will take time to implement, are a red flag. Our discussion also touched on the issue of inadequate IT and security resources, and the need to innovate the business. The point is, cybersecurity must be focused on what's important and cannot consume the entire budget.

Considering the value of cybersecurity insurance. One director brought up the importance of cybersecurity insurance coverage as a means to transfer some of the financial risk associated with a variety of cybersecurity incidents, including data breaches, business interruption, and network damage — particularly since the entity's directors and officers liability policy may not cover these issues. If a company invests in a cybersecurity policy, the insurer may require the business to follow certain guidelines and provide evidence through a cybersecurity assessment, as discussed earlier. If the company hasn't benchmarked itself against an appropriate framework, directors should inquire as to why not.