Cyber Insecurity: How Safe Can the Company's Data Assets Be?

KPMG's ACI Celebrating 15 Years

Cyber security is no longer just a technology concern, it has become a critical business issue, said Greg Bell, KPMG's National Practice Leader for Information Protection & Business Resilience, on KPMG's latest Quarterly Audit Committee Webcast. And while it has also moved much higher on board and audit committee agendas, oversight of cyber risk is clearly a major challenge for directors today.

According to KPMG's 2014 Global Audit Committee Survey, nearly 45 percent of U.S. audit committee members surveyed say their audit committee has primary oversight responsibility for cyber security risk; yet only 25 percent say the quality of the information they receive about cyber security is good.

Recent cyber security breaches in the headlines—including the theft of intellectual property, financial information and assets, and employee, client and customer data—have clearly sharpened the focus on cyber risk and the potential fallout: lost revenue, negative press and reputational damage, distraction to the business, regulatory/compliance issues, and, in some cases, national security concerns.

Of the audit committee members and other directors surveyed during the webcast, 14 percent said their company had experienced a "significant" cyber breach in the past 18 months.

Bell, along with Dennis Brixius, Chief Security Officer at The McGraw-Hill Companies, and webcast moderator James P. Liddy, KPMG LLP's U.S. Vice Chair of Audit, discussed key areas of focus for audit committees and board's in evaluating the company's cyber risk and readiness.

Cyber Risk Assessments "as a Matter of Course"

"Business is changing," said Greg Bell. "We are relying on a global set of partners and that requires us to rethink our approach to how information is accessed, stored and shared. Every company should be conducting cyber security risk assessments as a matter of course, identifying the most valuable digital assets and the greatest threats/risks to those assets." If the company has the right resources, such an assessment can be conducted internally; however, as cyber threats become more sophisticated, the company may need to consider an external specialist.

Fifty-one percent of directors surveyed during the webcast are concerned that mobile technology and social media have increased the company's vulnerability to cyber breaches. "There are so many ways to access and expose corporate information today that managing and protecting data and its use really comes down to basic security—confidentiality, integrity, and availability," said Brixius.

Weaving Cyber Security into the ERM Program

Cyber security requires a multi-disciplinary approach, integrated into the company's ERM processes and overall governance structure. Are the policies, responsibilities, and governance framework around cyber security clear and well communicated? What is internal audit's role? Is the company operating in-line with legal obligations, both in the US and abroad? Most importantly, are the company's cyber security efforts continuously improving as technology evolves and threats become more sophisticated?

The Scorecard

A robust cyber security scorecard—typically showing the volume, nature, and materiality of identified cyber incidents and how they are being managed; key cyber trends; and changes in the external environment—can help improve both the quality of cyber information and reporting, and the boardroom dialogue. "A good scorecard will develop over time and improve with every conversation," noted Bell.

Only 32 percent of audit committee members and other directors surveyed during the webcast said they had reviewed a dashboard or scorecard that management uses to monitor and manage cyber security risk.

Cyber Incident Response: Planning for the Inevitable

"It's no longer a matter of if, but when the company will have an incident or breach," said Bell. How would such a breach be communicated internally and externally and what specifically should be disclosed?

While 40 percent of directors surveyed during the webcast said their company has a clear cyber response plan in place, 22 percent said the company did not, and 38 percent were not sure.

Though every company has its own vulnerabilities and potential areas for disruption, the webcast dialogue highlighted the importance of scenario planning—involving all of the key players, including IT, risk, communications, legal, and policy teams—and establishing clear accountability: "Who is responsible for what in the event of a breach?" Lastly, what is the framework for making decisions on how to appropriately notify customers or third-parties?

Oversight of Cyber Risk: Considerations for the Board

- All data is not equal. Understand the value of the company's various data sets, and whether appropriate resources are devoted to securing the most critical assets.
- Conduct robust IT risk assessments periodically—and consider the need for an independent risk assessment.
- Recognize that most IT risk is internal "people" risk. How are we monitoring those risks?
- Requests regular cyber incident reports—a scorecard—to monitor cyber attacks and trends.
- Understand the company's cyber-incident response plan.

For more perspective on this topic, read **Global Boardroom Insights: The Cyber Security Challenge** *for views from six directors and executives from companies around the world*.

Financial Reporting and Regulatory Developments

Terry Iannaconi, a senior partner in KPMG's National Office, and former deputy chief accountant in the SEC's Division of Corporation Finance, provided an update on financial reporting developments and key considerations, including:

- Financial and risk disclosure continues to be top-of-mind. The FASB recently issued a disclosure framework concept release; the SEC is evaluating cyber security risk information as well as overall disclosure streamlining. KPMG also recently released a study on corporate disclosure from the perspective of institutional investors.

- Concerning FASB convergence projects—a final standard on revenue recognition is expected in the coming months, which would be effective December 15, 2016; on leases, both IASB and FASB remain committed to an approach that would require on-balance-sheet recognition, yet the boards are still apart on accounting models.

- Regarding PCAOB initiatives, the Board announced that it does not intend to pursue mandatory auditor rotation but continues to look for ways to enhance auditor independence.

Washington Update

Among notable developments from Washington, DC, Steven Walker, general counsel at the National Association of Corporate Directors, highlighted the SEC's continued focus on improvements to the corporate disclosure regime for the benefit of both companies and investors, as well recent commentary from Leo Strine, newly installed Chief Justice of the Delaware Court of Chancery, on limiting the frequency of say-on-pay votes and shortening the timeframe for activist investors to reveal their positions and motives.

For the full replay of the March webcast, visit KPMG.com/ACI.