Hot Topics
Cybersecurity… Continued in the boardroom

The **August 2013 Deloitte *Audit Committee Brief*** highlighted organizational roles and responsibilities for cybersecurity, beginning with the board of directors and audit committee. This month's *Hot Topics* article continues the discussion with further information on the board's role related to cybersecurity.

Not long ago, the term "cybersecurity" was not frequently heard or addressed in the boardroom. Cybersecurity was often referred to as an information technology risk, and management and oversight were the responsibility of the chief information or technology officer, not the board. With the rapid advancement of technology, cybersecurity has become an increasingly challenging risk that boards may need to address.

The board's role in the cyber world

A ***Carnegie Mellon University CyLab report*****,** as referenced in the August 2013 *Audit Committee Brief*, found shortcomings in board oversight of cybersecurity. The report, based on a survey of more than 100 board directors and senior executives at Forbes Global 2000 companies, compared the results of the 2012 survey with similar surveys conducted in 2008 and 2010.

The report stated, "For the third time, the survey revealed that boards are not actively addressing cyber risk management… There is still a gap in understanding the linkage between information technology (IT) risks and enterprise risk management. Boards still are not undertaking key oversight activities related to cyber risks, such as reviewing budgets, security program assessments, and top-level policies; assigning roles and responsibilities for privacy and security; and receiving regular reports on breaches and IT risks."

In addition to the questions noted in the August 2013 *Audit Committee Brief,* boards may consider asking themselves questions such as the following related to cybersecurity awareness:

- Is there someone on the board who serves as an IT expert and understands cyber risks?
- Does the company have cyber insurance?
- Is there a committee assigned to address cybersecurity?
- Does the company have a chief security officer who reports outside of the IT organization?
- Is social media a concern for our company?
- Do the outsourced providers and contractors have controls and policies in place and do they align with our company's expectations?
- Is there an annual company-wide education or awareness campaign established around cybersecurity?

The risk of cyber-attacks can directly affect both operations and the broader brand or reputation of a company, often resulting in significant financial repercussions. According to a 2012 Deloitte publication titled ***Risk intelligent governance in the age of cyber threats,*** the median annualized cybercrime-related cost in 2011 was $5.9 million, which was a 56 percent increase over the prior year. A primary responsibility of the board is to provide risk oversight. As discussed in the August 2013 *Audit Committee Brief*, the audit committee is often delegated the task of overseeing the risk programs and policies, including cybersecurity. The trend has been for other committees to be delegated the task of overseeing risks associated with their areas of expertise. For example, risks to the compensation plan might be overseen

by the compensation committee. Ultimately, however, the full board is accountable for risk oversight. In many instances, the committees are delegated the oversight of risk, however, the full board also discusses and continually monitors the most material risks and those for which the company is most vulnerable (i.e., where no controls exist to mitigate the risk). Typically when addressed, cybersecurity is a topic on the short list of risks and is typically discussed at the full board level rather than left solely with a committee.

Cybersecurity is a significant risk that can have a material impact. At least annually, boards should proactively ask questions of management, champion education and awareness programs company-wide, and treat risk as a priority. As cybersecurity issues increase and become more visible, boards may decide to take an active role in understanding the risks associated with those issues. Many boards hear from the chief information officer, chief technology officer, or others who are tasked with monitoring the cyber risk. In addition, some company boards are engaging third-party specialists to speak with them about the risk, how to mitigate it, and signs that may signal a breach. The full board take the necessary actions to stay informed on management's risk practices so it can effectively oversee cybersecurity.

Robert Mueller, director of the Federal Bureau of Investigation, recently spoke on a panel about the future of cybersecurity, said cyber threats will eventually equal or eclipse the terrorist threat. "There are only two types of companies—those that have been hacked and those that will be," Mueller said, adding that boards should ask themselves what type of company are they and what are they doing about it.

Concluding thoughts

Cybersecurity is a becoming top-of-mind issue for most boards, and directors are becoming more preemptive in evaluating cybersecurity risk exposure as an enterprise-wide risk management issue and not limiting it to an IT concern. The board plays a fundamental role in understanding the risks associated with cybersecurity and confirming preventative and detective controls are in place.

Additional Cybersecurity Resources

1. Cybersecurity and the audit committee, Audit Committee Brief, Deloitte LLP, August 2013
2. Preparing for Corporate Cyberattacks, The Corporate Board, September/October 2012
3. Risk Intelligent Governance in the Age of Cyber Threats: What you don't know could hurt you, Deloitte LLP, January 2012
4. Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions, Fischer, June 20, 2013
5. Carnegie Mellon Governance of Enterprise Security: CyLab 2012 Report, How Boards and Senior Executives are Managing Cyber Risks, Westby, May 16, 2012

Hot Topics articles are featured in each issue of *Corporate Governance Monthly*, a newsletter with the latest information for boards of directors and their committees from the Center for Corporate Governance (**www.corpgov.deloitte.com**).