Risk & Compliance Journal.
FROM THE WALL STREET JOURNAL

Deloitte.

Originally Published June 16, 2014, 12:01 AM ET

# For Audit Committees, a Growing Role in Cybersecurity

Numerous newsworthy events have kept cybersecurity at the forefront of board and audit committee agendas over the past several months. These include several high-profile retail breaches and, most recently, the discovery of the Heartbleed security vulnerability, which poses a major systemic challenge to securely storing and transmitting information via the Internet.

Mary Galligan, Director, Deloitte & Touche LLP

In addition, the government and regulators have been significantly increasing their focus on cyberthreats. The National Institute of Standards and Technology (NIST) released a Cybersecurity Framework in February 2014 in response to President Obama's 2013 executive order on enhancing critical cybersecurity infrastructure.

Additionally, the SEC's Office of Compliance Inspections and Examinations (OCIE) released a document in April 2014 that highlights sample questions and potential areas of informational requests that the OCIE may use in conducting examinations of registrants regarding cybersecurity. Though the guidance in the document is not intended to be comprehensive, it provides useful questions to consider regarding vulnerabilities and further demonstrates the attention senior government officials are devoting to cyberthreats.

"It is risky to view cybersecurity issues as purely compliance-related matters," notes Mary Galligan, former FBI Special Agent in Charge, Cyber and Special Operations, New York Office, and now a director with Deloitte & Touche LLP. "Compliance alone does not in itself imply an acceptable level of security."

## The Audit Committee's Role in Cybersecurity

The extent of the audit committee's involvement in cybersecurity issues varies significantly by company and industry. In some organizations, cybersecurity risk is tasked directly to the audit committee, while in others, there is a separate risk committee. Companies for which technology forms the backbone of their business often will have a dedicated cyberrisk committee that focuses exclusively on cybersecurity.

Regardless of the formal structure adopted, the rapid pace of technology and data growth, and the attendant risks highlighted by the recent security breaches demonstrate the increasing importance of understanding cybersecurity as a substantive, enterprise-wide business risk.

Audit committees should be aware of cybersecurity trends, regulatory developments and major threats to the company, as the risks associated with intrusions can be severe and pose systemic economic and business consequences that can significantly affect shareholders.

Engaging in regular dialogue with technology-focused organizational leaders can help the committee better understand where attention should be devoted. There are two foundational lines of questioning that audit committees may wish to keep in mind in overseeing cybersecurity risks:

—How do we know what data is leaving the company, and what associated monitoring activities are in place?

—Do we have a response plan for cyber incidents? Is it up to date and have we practiced it?

## Developing and Monitoring a Cybersecurity Plan

Cybersecurity plans should take into account the past, the present and the future with regard to cyberrisks. Consideration should be given to what percentage of the available budget should be devoted to prevention efforts, the immediate response to attacks and resiliency efforts. An effective cybersecurity plan incorporates the following questions:

—Secure: Are controls in place to guard against known and emerging threats?

—Vigilant: Can we detect malicious or unauthorized activities?

—Resilient: Can we act and recover quickly to minimize impact?

The SEC's cybersecurity disclosure guidance addresses the cybersecurity risks companies may need to disclose in their corporate filings, and such disclosures should be taken into consideration in developing and maintaining a cybersecurity program. The guidance can be a catalyst for modernizing information security programs and supporting business growth. Companies can gain a competitive advantage by following the SEC's guidance, as threats and vulnerabilities can be prioritized from a business growth and risk perspective.

Cybersecurity activities should extend beyond compliance efforts; a general IT audit is not a replacement for a full audit of cyber-related matters, as a general IT audit may not fully take into account the extent and pervasiveness of the associated risks.

## NIST's Cybersecurity Framework

The NIST's Cybersecurity Framework can help focus the conversation among the audit committee, other members of the board and senior management on what cybersecurity plans are in place and possible gaps. The framework has been developed through a continuing collaboration between the government and private industry. It offers guidance to assist organizations in voluntarily aligning specific cybersecurity practices with higher-level organizational strategies.

A key objective of the framework is to encourage organizations to consider cybersecurity risk as a priority similar to financial and operational risk when examining larger systemic risks to the organization. This can help bridge the gap between the seemingly technical world of cybersecurity and how it translates into the governance decisions that boards and senior executives make. It can also encourage dialogue between companies in similar industries which have a shared interest in identifying and addressing vulnerabilities.

The framework's core consists of five functions—identify, protect, detect, respond and recover—and related activities that provide a high-level, strategic view of an organization's management of cybersecurity risk and examine existing cybersecurity practices, guidelines and standards.

## Working with Law Enforcement

Governmental and other external interactions regarding cybersecurity are more frequent and arise sooner than many audit committees realize. As frequently as 40% of the time, companies first hear about breaches from outside organizations such as the FBI, a financial services provider or a telecommunications company, rather than through their own monitoring systems. When issues are raised through these means, the approach to dealing with the breach changes, as there may be requests for information, increased public exposure and the need for legal guidance.

Having an effective and demonstrable plan in place is all the more important when working with government agencies. Organizations can face requests by law enforcement to access their networks, and these requests frequently involve legal processes and inquiries from regulators and customers.

While addressing these issues, organizations must comply with various state data breaching laws and consider how best to communicate with shareholders and the public.

Given these sensitivities, companies are often reluctant to share nonrequired information with the government, but law enforcement entities often have information that companies do not, and thus it may be effective to develop a relationship with local and national government agencies so that the lines of communication are open in the event of an issue. Often, neither the government nor the company has the full picture of what has transpired, so it may be beneficial to fill in gaps by working together.

## Questions for Audit Committees to Consider as They Assess Cybersecurity Preparedness

Following are some questions that audit committees may consider asking management to assess the company's readiness to prevent and respond to cyberattacks:

—How do we know who is logging into our network, and from where?

—How do we track what digital information is leaving our organization and where it is going? Do we have an effective data loss prevention program?

—Which cyberthreats and vulnerabilities pose the greatest risk to the organization's business and reputation? What are the key assets to be protected? What is our strategy to address identified weaknesses?

—What systems are in place to protect information transferred through mobile technologies? Is there a culture of responsibility with regard to each employee's responsibilities in using mobile devices?

—Is management focused on making cyberrisk part of everyone's job, and not just IT's?

—Do we have the right gauges to measure the success of our cyberthreat management program?

—Are we planning to map our policies to the NIST Framework? If we are already following an industry-recognized standard, how much effort would it take to map the steps we have already taken to the framework?

—What are our training programs to educate our workforce about cyberrisks and responsibilities?

## Looking Ahead

Increasingly, cybersecurity is becoming a 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 will continue to play a fundamental role in understanding the risks associated with cybersecurity and confirming preventative and detective controls are in place.

### Related Resources

Audit Committee Brief—Technology at the Forefront
The Board's Role in Overseeing Cybersecurity Risk
Highlights of the SEC's Cybersecurity Roundtable
As Cyberattacks Evolve, So Should the Corporate Response
Fighting Cybercrime with Public, Private Cooperation
Cyberrisk: What Lessons Have We Learned?
How Companies Can Apply the SEC's Cybersecurity Disclosure Guidance
Rising Cyberrisks at the Center of New Security Standards