Deloitte.

Heads Up

April 8, 2014
Volume 21, Issue 9

In This Issue:


- Cybersecurity Executive Order and Framework
- Cybersecurity Landscape
- Public-Company Disclosures
- The Role of the Board of Directors and Senior Leadership
- Best Practices
- Next Steps


SEC Chairman Mary Jo White highlighted that cybersecurity threats are global and pose a grave risk to our economy, including "our critical infrastructures, our financial markets, banks, intellectual property, and . . . the private data of the American consumer."

# Cyber Chat

# Highlights of the SEC's Cybersecurity Roundtable

*by Joe DiLeo and Lyndsey McAlister, Deloitte & Touche LLP*

On March 26, 2014, the SEC hosted a roundtable on cybersecurity and the related challenges for market participants (e.g., public companies, broker-dealers, investment advisers, and transfer agents). In her opening remarks, SEC Chairman Mary Jo White highlighted that cybersecurity threats are global and pose a grave risk to our economy, including "our critical infrastructures, our financial markets, banks, intellectual property, and . . . the private data of the American consumer." She noted that these risks are "first on the Division of Intelligence's list of global threats, even surpassing terrorism." Panelists from a wide array of backgrounds, including government officials, professional service providers, academics, investors, preparers, and market exchange representatives, shared their experiences with evaluating and addressing these cybersecurity challenges.

This *Heads Up* highlights three key topics discussed at the SEC's roundtable: (1) the current cybersecurity landscape, (2) public-company disclosure issues, and (3) the role of the board of directors and senior leadership in assessing and responding to cybersecurity threats. This publication also summarizes cybersecurity-related guidance and panelists' observations about best practices that companies could consider in preparing for and responding to cyberattacks.

## Cybersecurity Executive Order and Framework

As a prelude to their observations, numerous panelists referred to President Obama's February 2013 executive order on cybersecurity, *Improving Critical Infrastructure Cybersecurity*, and the National Institute of Standards and Technology (NIST) cybersecurity framework, *Framework for Improving Critical Infrastructure Cybersecurity*.

The executive order was issued to communicate the "policy of the United States to enhance the security and resilience" of the nation's critical infrastructure[1] and protect it from cyberthreats. The executive order's requirements include (1) more timely sharing of cyberthreat-related information between U.S. government agencies and with private-sector companies; (2) development of a "baseline" framework to reduce cybersecurity risks; (3) establishment of a voluntary critical infrastructure cybersecurity program to support the adoption of the cybersecurity framework; and (4) identification of the critical infrastructure that is subject to the greatest risk.

**Editor's Note:** The Department of Homeland Security (DHS) has identified 16 critical infrastructure sectors. For each sector, the DHS provides a summary, a sector-specific plan, and other resources. In discussing the sectors in relation to the current cybersecurity landscape, one panelist noted that the financial services and energy sectors are subject to the most attacks.

[1] The executive order defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

In response to the executive order, NIST released the first version of its cybersecurity framework in February 2014. The framework outlines what NIST believes is a strategic, cost-effective approach to managing cybersecurity-related risks. According to NIST, the framework "focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of [an] organization's risk management processes." The framework is intended for use by all companies, regardless of their size or complexity, and contains risk management principles (and best practices) that would allow companies to improve "the security and resilience of critical infrastructure." However, NIST cautions companies that the framework is not a "one-size-fits-all" approach for dealing with cybersecurity risks.

**Editor's Note:** On March 21, 2014, the CAQ issued an alert that highlights the independent external auditor's cybersecurity responsibilities. The alert, which was issued before the roundtable to help panelists prepare for the discussion, summarizes cybersecurity-related audit procedures performed in both audits of financial statements and ICFR, "including evaluating the risks of material misstatement to a company's financial statements resulting from unauthorized access" to financial reporting systems.

## Cybersecurity Landscape

Panelists described the various types of cyberattack perpetrators, as well as their methods and motivation for carrying out the attacks. One panelist likened the rapid evolution of threats to a game of "whack-a-mole," since a new cyberthreat often arises as soon as another threat is struck down.

Panelists described the various types of cyberattack perpetrators, as well as their methods and motivation for carrying out the attacks.

A key theme at the roundtable was that cyberthreats may affect not only technology but also an entity's broader operations. Mary Galligan, director of Cyber Risk Services at Deloitte & Touche LLP, outlined a three-pronged "threat matrix": (1) threat vectors, (2) threat intelligence, and (3) threat resiliency. Threat vectors encompass cyberattack perpetrators and the reasons for their attacks. Threat intelligence involves an acknowledgment that securing data is not sufficient and that information sharing with governmental and other private-sector parties is also needed. Threat resiliency — or an entity's ability to quickly identify, remediate, and recover from incidents — is critical because a cyberattack often increases the risk of other threats. Such additional threats include disruption of an entity's daily business operations, damage to its reputation (not only from the attack itself but from public reception of the entity's disclosures about the attack), and the costs of responding to and remediating a cyberattack.

Panelists classified perpetrators of cyberattacks (and the motivations behind their attacks) into the following broad categories:

- *Nation-states and spies* — Those that seek to steal national security secrets or intellectual property.
- *Organized criminals* — Perpetrators that use sophisticated tools to steal money and private or sensitive information about an entity's consumers (e.g., identity theft).
- *Terrorists* — Those that look to attack key economic infrastructure in the United States.
- *"Hacktivists"* — Individuals or groups that want to make a social or political statement by stealing or publishing an organization's sensitive information.

Some panelists emphasized that an organization's insiders pose a risk because of their intimate knowledge of, and access to, key systems and operations. In particular, panelists warned entities about "bad leavers" (i.e., individuals whose employment with an entity is terminated). Panelists also discussed the cybersecurity risks resulting from (1) relationships with third parties (e.g., customers, vendors, or subcontractors) that have physical access to an entity's systems or whose systems may access the entity's systems but be vulnerable to cyberattacks, (2) overseas operations, and (3) employees that can access an entity's systems through mobile devices.

Some of the methods used to carry out cyberattacks include destruction of infrastructure, denial of service, "ransomware" (i.e., encrypting files until a ransom is paid), and theft. Panelists gave various examples of these cybersecurity breaches, including a broker-dealer relationship in which a broker's system is breached and fraudulent transactions are executed. Another example involved attempts to take over individual accounts of investment advisers' wealth management clients. In addition, various phishing schemes were discussed, including ones in which the attacker poses as a vendor or customer and sends a fraudulent e-mail to an entity's employee that requests (1) confirmation of account information or (2) that funds be remitted to an improper account. In some cases, such e-mails appear to have originated from another employee.

Entities were urged to look beyond threats, methods, perpetrators, and their motivations and were advised to assess vulnerabilities to cyberattacks in their systems. One panelist observed that cyberincidents have evolved from random and haphazard occurrences to thorough and methodical attacks. Such attackers patiently wait to expose an entity's vulnerabilities and, once they gain access to the entity's system, are persistent.

## Public-Company Disclosures

In October 2011, the SEC's Division of Corporation Finance issued CFDG Topic No. 2, *Cybersecurity*,[2] in response to an increase in cybersecurity incidents, some of which caused certain companies to incur significant remediation and other costs for (1) direct damages (both real and reputational), (2) impacts on their customers, and (3) increased protection from future cybersecurity attacks.

Elaborating on materiality, panelists described the challenge of applying materiality concepts to cybersecurity disclosures, which often describe incidents with significant qualitative elements or for which the quantitative impact is not yet known.

The Commission asked panelists about the effectiveness of current cybersecurity-related disclosure guidance. Certain panelists noted that many of the current cybersecurity-related disclosures are "boilerplate" and repeat words from CFDG Topic 2 rather than being tailored to the registrant. Other panelists, however, described the potential risks of providing tailored disclosures. Some expressed concerns that more specific disclosures could increase a company's vulnerability since they might include details that help attackers infiltrate the company.

Panelists explained that an entity may learn of a cybersecurity breach from organizations such as the FBI or DHS. Because the information breached is confidential, an entity may not be able to disclose the cyberincident. In the spirit of promoting the information sharing that President Obama's executive order calls for, one panelist asked the Commission and other federal agencies to ensure that they are communicating with one another when a registrant has been breached. Panelists noted that effective interagency communication would alleviate circumstances in which one agency may ask a registrant for more disclosure yet another may tell the registrant not to disclose an incident.

**Editor's Note:** As highlighted in its recent "SEC Speaks in 2014" conference, the SEC staff acknowledged that entities often need to strike a balance between disclosing information related to cybersecurity breaches and creating a "roadmap" for potential cyberattacks by providing detailed disclosures, especially when a registrant is cooperating with authorities in an investigation. The SEC staff also encouraged registrants to practice "disclosure efficiency" by avoiding boilerplate cybersecurity disclosures and instead tailoring their disclosures to include (1) the aspects of the business that are subject to risks, (2) updates for new information, and (3) cost estimates, if possible and material. See Deloitte's March 20, 2014, *Heads Up* for more information on the "SEC Speaks in 2014" conference.

Panelists also observed that disclosures about immaterial events would not be meaningful for investors and may heighten a company's exposure to litigation. Elaborating on materiality, panelists described the challenge of applying materiality concepts to cybersecurity disclosures, which often describe incidents with significant qualitative elements or for which the quantitative impact is not yet known. One panelist explained

[2] CFDG Topic 2 provides interpretive guidance about potential disclosures related to material cybersecurity matters. According to the SEC staff's guidance, entities must address considerations related to disclosure in a registrant's (1) financial statements, (2) risk factors, (3) legal proceedings, and (4) disclosure controls and procedures.

that often state legislation focuses on security breaches that affect customer information and results in low thresholds for the disclosures that an entity needs to provide when there are breaches in the entity's system. The result is that entities often provide granular disclosures about immaterial breaches — a fact that one panelist believed is supported by data showing small declines in registrants' stock prices after cyberincidents are disclosed or short-term recoveries in stock prices when stocks decline more significantly.

**Editor's Note:** While the SEC has not yet decided whether it will provide additional guidance on cybersecurity disclosure requirements, panelists indicated that they generally prefer principles-based rulemaking to prescriptive rulemaking, which may become obsolete because of the developing nature of the risks. In summarizing the panel discussion, SEC Commissioner Kara Stein asked whether the Commission had provided sufficient cybersecurity disclosure guidance to registrants. She elaborated by asking panelists whether "minimum standards" for cybersecurity disclosures are necessary — or even possible given the various types of registrants. Ms. Stein highlighted that panelists consistently talked about using a multidimensional approach to address cybersecurity threats. She suggested that the Commission might need to be "dynamic in [its disclosure] requirements" and that such an approach may promote disclosures that are meaningful to investors yet not overly burdensome to registrants.

## The Role of the Board of Directors and Senior Leadership

Panelists suggested that the board of directors and senior leadership are critical to the effectiveness of a company's preparedness for and resilience to cybersecurity threats.

One panelist noted that approximately 1 percent of boards of directors have a member with cybersecurity or technology expertise. This statistic prompted a question from Chairman White soliciting panelists' feedback about who is responsible for cybersecurity matters within entities' governance structures. Panelists indicated that this varies but that, at many companies, audit or risk committees have such responsibilities. Some organizations have formed cybersecurity committees. One panelist noted that entities with complex supply chains or multifaceted sales-delivery models could have separate cybersecurity committees for different aspects of their IT infrastructures.

While an increasing number of boards are engaging outside experts for assistance with evaluating cybersecurity risks, panelists did not believe that entities should be required to have (1) a separate cybersecurity committee or (2) a dedicated expert on the board or one of its committees. Instead, panelists suggested that the board of directors and senior leadership are critical to the effectiveness of a company's preparedness for and resilience to cybersecurity threats. As for how they are expected to perform their governance responsibilities in relation to cybersecurity risks, individuals in an entity's governance structure (and other leadership roles) need to be able to ask the right questions, understand the strategic implications of threats, and focus on the long-term proficiency of the entity's protocols and response program.

## Best Practices

At various points throughout the event, panelists shared what they believed to be best practices for addressing cybersecurity risks in organizations. The discussion of best practices included topics such as culture, monitoring and information sharing, and cybersecurity planning.

### Culture

Many panelists agreed that simply implementing an IT solution or certain internal controls was not enough to address continuously changing cybersecurity threats. Some panelists suggested that prevention of cyberattacks starts with diligence in the hiring process, including proper background checks. In addition, panelists emphasized that all employees in an organization own the cybersecurity risk together and that organizations must have a strong "tone at the top" with respect to vigilance regarding such matters.

One panelist expressed the belief that senior management can play an important role in creating a cybersecurity culture that "starts at the keyboard" and in which cybersecurity is not seen as a technology issue for the IT department to resolve but a business issue in which all employees take action and understand their role in protecting their company's information.

## Continuous Monitoring and Information Sharing

Panelists encouraged companies to engage in continuous monitoring activities, including extensive threat modeling, periodic system testing, gap analysis, risk management, and recovery planning. Another common best practice that panelists suggested was incursion testing to ensure that employees understand their responsibilities to safeguard the company's data and operational integrity. Incursion testing includes vulnerability tests such as sending employees phony phishing e-mails, leaving voicemails requesting employees to change their passwords, and placing a flash drive with malware in a common area to test whether any employees load the phony malware onto their computers.

Given the ever-changing nature of cyberthreats, panelists reiterated that information sharing is of paramount importance. However, panelists recognized that information about cyberattacks is sensitive (if not classified) and that entities may encounter barriers in sharing such information. These barriers may include (1) unclear channels or forums in which to share the information or (2) personnel who do not have the appropriate security clearance to obtain classified information from the government. However, panelists encouraged continued improvements in information sharing because the sooner an incident is detected and described to other organizations, the faster (1) organizations can respond to, and recover from, similar attacks and (2) market and economic disruptions can be reduced.

Many panelists agreed that companies should concentrate on the most vulnerable aspects of their operations.

## Cybersecurity Planning, Protocols, and Controls

Panelists explained that cybersecurity risk cannot be addressed by a one-time IT solution but must be evaluated on an ongoing basis and that entities need to attempt to mitigate cybersecurity risks in a manner similar to other business risks. Consequently, companies must continually evaluate their vulnerabilities related to business processes and key systems. Given companies' limited resources and the scarcity of cybersecurity resources, many panelists agreed that companies should concentrate on the most vulnerable aspects of their operations rather than focusing too broadly on systemic risk. When resources are stretched too thin, no vulnerabilities are sufficiently covered, leaving a company at greater risk. In assessing a company's vulnerabilities, Ms. Galligan summarized questions that a company should consider asking:

- How should protection be prioritized? What information really needs to be protected (i.e., a risk assessment should be performed)?
- How should access to systems be managed, especially third-party access?
- How are findings related to monitoring efforts evaluated (i.e., does the company have sufficient resources with appropriate expertise to effectively review the results and findings of monitoring activities)?

Many panelists stressed the importance of establishing a response and recovery plan and practicing the plan so that employees are aware of how to respond before an attack occurs. An effective cybersecurity recovery plan should also be continually updated by and with key stakeholders.

Companies were also advised to create an appropriate escalation framework that includes well-defined thresholds for reporting cybersecurity incidents to senior leadership, committees of the board of directors, and the board of directors itself. Because the quantitative impact of these threats may not be clear initially, panelists recommended that such thresholds be flexible enough to take into account the varying nature of cyberincidents.

## Next Steps

In addition to obtaining feedback from panelists, the SEC asked constituents to share their input online. The SEC plans to analyze the information obtained from the panels and other interested parties and will consider taking additional measures — including evaluating the effectiveness of previously issued guidance. In addition, in his prepared remarks, SEC Commissioner Luis Aguilar recommended that the Commission create a Cybersecurity Task Force in the near term to discuss issues identified and make recommendations to the Commission.

## Subscriptions

If you wish to receive *Heads Up* and other accounting publications issued by Deloitte's Accounting Standards and Communications Group, please register at www.deloitte.com/us/subscriptions.

## *Dbriefs* for Financial Executives

We invite you to participate in *Dbriefs*, Deloitte's webcast series that delivers practical strategies you need to stay on top of important issues. Gain access to valuable ideas and critical information from webcasts in the "Financial Executives" series on the following topics:

- Business strategy and tax.
- Driving enterprise value.
- Financial reporting.
- Financial reporting for taxes.
- Governance and risk.
- Technology.
- Transactions and business events.

*Dbriefs* also provides a convenient and flexible way to earn CPE credit — right at your desk. Subscribe to *Dbriefs* to receive notifications about future webcasts at www.deloitte.com/us/dbriefs.

Registration is available for this upcoming *Dbriefs* webcast. Use the link below to register:

- Quarterly Accounting Roundup: An Update on Important Developments (June 25, 2 p.m. (EDT)).

## Technical Library and US GAAP Plus

Deloitte makes available, on a subscription basis, access to its online library of accounting and financial disclosure literature. Called Technical Library: The Deloitte Accounting Research Tool, the library includes material from the FASB, the EITF, the AICPA, the PCAOB, the IASB, and the SEC, in addition to Deloitte's own accounting and SEC manuals and other interpretive accounting and SEC guidance.

Updated every business day, Technical Library has an intuitive design and navigation system that, together with its powerful search features, enable users to quickly locate information anytime, from any computer. Technical Library subscribers also receive *Technically Speaking,* the weekly publication that highlights recent additions to the library. For more information, including subscription details and an online demonstration, visit www.deloitte.com/us/techlibrary.

In addition, be sure to visit US GAAP Plus, our new free Web site that features accounting news, information, and publications with a U.S. GAAP focus. It contains articles on FASB activities and updates to the *FASB Accounting Standards Codification*™ as well as developments of other U.S. and international standard setters and regulators, such as the PCAOB, the AICPA, the SEC, the IASB, and the IFRS Interpretations Committee. Check it out today!