Wall Street LAWYER
Securities in the Electronic Age
May 2014 ■ Volume 18 ■ Issue 5

Implications of the SEC's Increased Focus on Cybersecurity

BY RYAN BERGSIEKER

Ryan Bergsieker, a former federal computer crimes prosecutor, is Of Counsel in the Denver office of Gibson, Dunn & Crutcher LLP. Contact: rbergsieker@gibsondunn.com.

On April 15, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert describing its plans to review the cybersecurity preparedness of at least 50 registered broker-dealers and investment advisors.[1] The Risk Alert is merely the latest in a string of recent announcements from the SEC regarding its increased focus on cybersecurity. Together, these announcements suggest that all regulated firms should prepare for greater scrutiny in this area. Indeed, there is every indication that the SEC will follow up on these initial examinations by issuing more detailed guidance on cybersecurity, and may move toward enacting new regulation in this area.

The April 15 Risk Alert

Precursors to the April 15 Risk Alert

The SEC began 2014 by announcing that its examination priorities for the year would include a focus on technology, including topics related to cybersecurity preparedness.[2] Specifically, the SEC included a range of cybersecurity issues as examination priorities, including governance and supervision of information technology systems, information security, and preparedness to respond to sudden malfunctions and system outages.

Following the announcement of its examination priorities in early 2014, on March 26 the SEC sponsored a Cybersecurity Roundtable. In his remarks at the Roundtable, SEC Commissioner Luis Aguilar emphasized the importance of the SEC gathering additional information and "consider[ing] what additional steps the Commission should take to address cyber-threats."[3] The Roundtable provided private and public sector representatives an opportunity to discuss cybersecurity generally, with a focus on the specific cyber-risks faced by regulated entities and public companies. Not coincidentally, it also provided the SEC an opportunity to develop a better understanding of participants' growing concern over cybersecurity threats.

The Roundtable provided private and public sector representatives an opportunity to discuss cybersecurity generally, with a focus on the specific cyber-risks faced by regulated entities and public companies.

Several themes emerged during discussions at the Roundtable:

- *Cybersecurity will be an Ongoing Challenge*—Multiple speakers emphasized that cybersecurity threats should not be viewed as problems that can be

completely resolved, but rather as risks that must be managed and mitigated in the same manner as other operational risks companies face.

- ***Information Sharing is an Important Tool to Address Cybersecurity Threats***—The panelists at the Roundtable agreed that information sharing—between industry participants, as well as through public-private partnerships—can be an important resource for combating cybersecurity challenges.

- ***The Board of Directors and Senior Management Have an Important Role to Play***—According to the Roundtable panelists, after years of considering cybersecurity risk management as the sole domain of information technology personnel, senior management and boards are realizing that cybersecurity should be ranked highly on their priority lists, and studies show an increasing level of awareness of the cybersecurity risks faced by companies today. While the role of leadership—and the cyber-expertise expected of leadership—will vary depending on the nature of the company, the panelists generally agreed that cybersecurity should not be viewed as a technology issue, but rather as a business issue.

Content of the April 15 Risk Alert

The April 15 Risk Alert states that the OCIE's cybersecurity initiative "is designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats."[4] The Alert goes on to state that the planned examinations will focus generally on

> **the entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats.[5]**

Finally, the Alert emphasizes that the examinations "will help identify areas where the Commission and the industry can work together to protect investors and our capital markets from cybersecurity threats."[6]

In addition to providing an overview of the number of examinations it will perform and the general focus of those examinations, the Alert provides a sample request for information and documents used as part of these examinations. According to the Alert, this unusual move is "intended to empower compliance professionals in the industry with questions and tools they can use to assess their firms' level of preparedness, regardless of whether they are included in OCIE's examinations."[7]

> ***The Alert is silent on what consequences firms that do not perform well on the SEC's tests may face.***

The sample request for information and documents contains 28 detailed questions.[8] Some of the requests track material in the National Institute of Standards and Technology (NIST) cybersecurity framework, which was published in February 2014.[9] Others are much more specific, calling for detailed information on policies, procedures, personnel and past events.

The Alert is silent on what consequences firms that do not perform well on the SEC's tests may face. However, deficiency letters or even referral for enforcement are possibilities, based on past Commission practice.

Analysis of the April 15 Risk Alert

Several themes emerge from the April 15 Risk Alert:

- ***The Alert is Intended to Have an Outsized Impact***—As part of the Cybersecurity Initiative announced in the April 15 Alert, the SEC will examine only a tiny fraction of the approximately 4,500 registered broker-dealers and more than 10,000 registered investment advisors. By publicizing the initiative, however, and especially by taking the unusual step of publicizing a detailed and wide-ranging sample set of information and document requests, the SEC is taking steps to broaden

the impact of the Initiative. The SEC's clear intent is for compliance professionals at the many firms where it is not conducting examinations to conduct a rigorous self-examination—and move to remediate any deficiencies they discover.

- ***Responding After a Breach***—The questions in the sample information and document request lay out a roadmap of the issues the SEC appears to believe firms should at least consider in the area of cybersecurity preparedness. Firms that do suffer a breach should expect the SEC—and perhaps other regulators—to ask, not just about how the firm is responding to the breach, but also about what measures the firm took to prevent it from happening in the first place.

- ***The SEC is Focused on All Aspects of Data Security***—The sample information and document request appended to the April 15 Alert is very broad. Previously, much of the SEC's focus was on protecting the privacy of customers' personal information. This Alert makes clear that the SEC's new focus is far more comprehensive.

- ***In the Absence of Comprehensive Regulation, Voluntary Frameworks Increase in Importance***—The NIST cybersecurity framework is ostensibly nothing more than a voluntary framework companies in certain critical infrastructure segments may use to identify and mitigate their cybersecurity risk. However, the SEC refers to it repeatedly in the sample set of information and document requests appended to the April 15 Alert, demonstrating that in the absence of comprehensive regulation, voluntary frameworks like that from the NIST may take on increased importance as benchmarks for liability purposes. It is crucial for regulated entities, like other businesses, to be familiar with such frameworks.

- ***The Details Matter***—Much of the cybersecurity guidance offered by the federal government to date has been focused at a high level of generality. For example, the NIST cybersecurity framework is focused on high-level risk management processes. The SEC's Risk Alert adopts this framework, but goes beyond it to emphasize the details of cybersecurity preparedness: device and systems inventories, resource maps, catalogs of network collections, logging capabilities, malware controls, data segregation, and event detection processes, to name just a few.

- ***Documentation is Crucial***—The sample information and document request contains multiple questions focused on policies and procedures. However, it goes beyond these questions to focus on the dates and results of periodic risk assessments, penetration tests and more. Preserving adequate documentation related to cybersecurity in known locations will make it far easier to respond to the SEC during a routine or other examination. Firms can no longer simply adopt a data security policy and hope for the best when it comes to record-keeping; instead, companies must carefully document their implementation of such policies.

- ***The SEC's Focus is on Real-World Problems***—Several of the questions in the sample information and document request closely track areas where major problems have arisen in the past year. The SEC's focus on the risks associated with vendors and third parties mirrors the large-scale data breach at Target Corp. in late 2013, where the breach allegedly was facilitated by unauthorized systems access at a Target vendor. The SEC's focus on remote customer access mirrors concerns about the Heartbleed vulnerability, which, while it was announced after the SEC's publication of its Risk Alert, is the latest iteration by which hackers may attempt to gain login information used in transactions like these. And the SEC's focus on the detection of unauthorized activity mirrors problems at many companies and institutions that have been the target of a data breach, and yet may not have detected the breach until informed about it months later by law enforcement or others.

Conclusion: The Time for Action is Now

The SEC has stated that cybersecurity is an important priority for its examinations. In the sample information and data request it attached to the April 15 Alert, the SEC provided compliance professionals a

helpful tool to begin a rigorous self-examination process. The carrot has been offered, and the stick may not be far behind.

The carrot has been offered, and the stick may not be far behind.

Broker-dealers and investment advisors should consider (*i*) carefully evaluating their existing cybersecurity policies and practices in light of the extensive set of questions contained in the SEC's sample information and data request; and (*ii*) making any necessary adjustments in advance of routine examinations. While broker-dealers and investment advisors are the specific focus of the April 15 Alert, other regulated entities should consider taking similar steps: just as the SEC's focus is not limited to a single aspect of data security, so too is its industry focus not likely to be limited to a handful of sectors.

NOTES

1. OCIE Cybersecurity Initiative, *available at* http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.
2. Examination Priorities for 2014, *available at* http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf.
3. Commissioner Luis A. Aguilar, "The Commission's Role in Addressing the Growing Cyber-Threat," Statement at SEC Roundtable on Cybersecurity (March 26, 2014), *available at* http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184.
4. OCIE Cybersecurity Initiative, at 2.
5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.*, at Appendix.
9. *See* Alexander H. Southwell, Ryan T. Bergsieker & Stephenie Gosnell Handler, *The Cybersecurity Framework: Risk Management Process... and Pathway to Corporate Liability?*, Westlaw J. Computer & Internet (Dec. 12, 2013).