UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

38th Annual Conference on Securities and Business Law

February 11-12, 2016
Dallas, Texas

Cybersecurity in 2016

Marshall M. Gandy

Richard J. Johnson

Chad M. Pinson

MATERIALS PREPARED FOR

38th Annual Conference on Securities and Business Law

A Checklist for Responding to SEC Cybersecurity Audits

The views set forth herein and in the accompanying presentation are the personal views of the speaker and do not necessarily reflect those of the law firm with which he is associated, the SEC, or Stroz Friedberg.

FEBRUARY 11-12, 2016

SEC Cybersecurity Audits

On September 15, 2015, the Office of Compliance Inspections and Examinations ("OCIE") within the U.S. Security and Exchange Commission ("SEC") issued a "Risk Alert" highlighting the cybersecurity risks and issues that need to be addressed by registered broker-dealers, investment companies, and investment advisers. *See* OCIE, NEP Risk Alert, OCIE Cybersecurity Examination Initiative (Sept. 15, 2015), *available at* https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf. Registered entities that fail to implement any necessary changes in light of this guidance could be subject to regulatory enforcement proceedings and substantial penalties. The SEC has signaled a growing willingness to sanction registered firms for inadequate cybersecurity policies and procedures. *See In the Matter of R.T. Jones CapitalEquities Management, Inc.* (Sept. 22, 2015), *available at* http://www.sec.gov/litigation/admin/2015/ia-4204.pdf. Moreover, SEC Commissioner Aguilar stated earlier this year that "the SEC has been proactively examining how it can bring more cybersecurity enforcement actions using its existing authority, and how that authority might need to be broadened to meet emerging cybersecurity threats." SEC, A Threefold Cord – Working Together to Meet the Pervasive Challenge of Cyber-Crime (June 25, 2015), *available at* http://www.sec.gov/news/speech/threefold-cord-challenge-of-cyber-crime.html.

In its Risk Alert, OCIE announced a "second round of cybersecurity examinations" that will "involve more testing to assess implementation of firm procedures and controls," and it identified the following cybersecurity priorities on which SEC examiners will focus in upcoming examinations of registered entities:

- Governance and Risk Assessment
- Access Rights and Control
- Data Loss Prevention
- Vendor Management
- Training
- Incident Response

OCIE examiners will review firms' written policies and procedures with respect to these "key topics" and will request an exhaustive list of documents and information in accordance with the "Document Request List" that was included as an appendix to the Risk Alert.

- - - - - - - - - - - - -

We recommend that registered broker-dealers, investment companies, and investment advisors immediately (1) assess their policies, procedures and systems in relation to the six cybersecurity priorities described above and (2) implement any necessary changes in light of the SEC's guidance. The following checklist may serve as a useful guide for doing so.

Checklist – SEC Cybersecurity Audits

I. GOVERNANCE AND RISK ASSESSMENT

Examiners may assess whether SEC registrants have cybersecurity governance and risk assessment processes relative to access rights and controls; data loss prevention; vendor management; training; and incident response. Examiners also may assess whether firms are periodically evaluating cybersecurity risks and whether their controls and risk assessment processes are tailored to business operations. Furthermore, Examiners may review the level of communication to, and involvement of, a registrant's senior management and/or board of directors. Registered entities should have internal policies and procedures in place for managing cybersecurity risk.

A. Provide in Advance

- ☐ **Written Policies and Procedures – Information Security:** Does the registrant have information security policies and procedures in place that address the protection of customer non-public information ("NPI") against anticipated threats and unauthorized access?

- ☐ **BOD/Senior Management Involvement:** Does the registrant have Board of Directors ("BOD") minutes and/or briefing materials regarding the following cybersecurity-related issues: risks, incident response planning, actual incidents, and vendor-related matters?

- ☐ **CISO:** Does the registrant have a Chief Information Security Officer ("CISO") or equivalent position? If not, does the registrant have an individual or department with principal responsibility for overseeing cybersecurity-related matters?

B. Make Available On-Site

- ☐ **Organizational Roles and Responsibilities:** Does the registrant have defined roles and responsibilities for cybersecurity-related matters throughout the organization? Can the registrant provide documents—such as organizational charts or similar materials—that describe these roles and responsibilities and where they fall along the corporate hierarchy?

- ☐ **Periodic Risk Assessments:** Does the registrant conduct periodic risk assessments to identify cybersecurity threats and vulnerabilities as well as potential business consequences? Can the registrant provide documentation of the most recent assessment, including the scope of the review, any moderate or high risks identified, and remediation efforts implemented?

- ☐ **Penetration Testing:** Does the registrant have written policies and procedures in place related to penetration testing (whether separate or part of a larger information security policy)?

Title search: Cybersecurity in 2016

Also available as part of the eCourse
Cybersecurity Update for Securities Practitioners

First appeared as part of the conference materials for the
38th Annual Conference on Securities and Business Law session
"Cybersecurity in 2016"