Brian Hoffman

Partner
303.295.8043
Denver, Washington, DC
bnhoffman@hollandhart.com

SEC Urges "Robust" Cybersecurity Best Practices

Insight — 08/22/2017

As cyber-attacks continue to threaten the financial industry, the SEC has made cybersecurity an urgent priority. On August 7, the SEC's Office of Compliance Inspections and Examination (OCIE) released a new cybersecurity Risk Alert. This Risk Alert provides valuable insights into entities about effective cybersecurity practices. Entities and their personnel are well-advised to refresh their cybersecurity policies, practices, and training in light of the matters flagged in this Risk Alert.

The Risk Alert describes findings from OCIE's second cybersecurity survey of 75 regulated entities (registered broker-dealers, investment advisers, and investment companies), based on examinations conducted between September 2015 and June 2016. OCIE's first survey was conducted in 2014, and published in 2015. Underscoring the SEC's keen focus on cybersecurity concerns, this is the SEC's fifth release focused on cybersecurity since 2014.

OCIE's Risk Alert contains a mixed progress report on firms' cybersecurity practices, as well as some important best practices for "robust" cybersecurity.

Good News / Bad News Progress Report

The recent survey includes some good news, as well as highlights areas for improvement for firms. Overall, OCIE found significant improvements in cybersecurity preparedness since its first initiative. Yet in certain key areas, OCIE's recent survey revealed a mixed bag:

- **Policies and Procedures:**
    - Most firms maintained written policies and procedures relating to the protection of confidential information, as well as addressing Regulation S-ID, aimed at preventing identity theft; and Regulation S-P, which covers the privacy of consumer financial information.
    - Yet some firms' policies and procedures were not reasonably tailored to the firm, and actual practices did not always adhere to the written policies and procedures.
- **System Maintenance:**
    - Most firms had a process in place for ensuring regular system maintenance, including the installation of software patches to address security vulnerabilities.
    - Some firms lagged in installing a significant number of system patches, including critical security updates designed

to address vulnerabilities.

- **Risk Assessments:**
  - Most firms conducted periodic risk assessments, including penetration tests and vulnerability scans on systems that the firms considered to be critical, to identify cybersecurity threats, vulnerabilities, and the potential business consequences of a cyber incident.
  - A number of firms used outdated risk assessments, and did not appear to fully and quickly remediate some high risk observations that they discovered from these tests and scans.
- **Vendor Assessments:**
  - Almost all firms conducted vendor risk assessments or required that vendors provide reports on their security risks and remediation.
  - Many firms did not require updates to the initial assessments on at least an annual basis.
- **Incident Monitoring and Response:**
  - All firms used systems or tools to prevent, detect, and monitor for leaks of personally identifiable information.
  - Most firms had plans for addressing access incidents, as well as specifically delineated roles and responsibilities for cybersecurity matters.
  - Although some firms lacked clear plans for data breach incidents and most had plans for notifying customers of material events.

Best practices

In the Risk Alert, OCIE also identifies certain hallmarks of "robust" cybersecurity policies and procedures. Although not a comprehensive list, OCIE recommended that firms use these best practices as a check list when assessing the adequacy and effectiveness of their own cybersecurity compliance programs. OCIE suggested that firms:

- Maintain a complete inventory of data, information, and vendors, along with classification of risks;
- Create detailed cybersecurity-related instructions connected to penetration tests, security monitoring and system auditing, access rights, and reporting;
- Maintain prescriptive schedules and processes for testing the integrity and vulnerabilities of data;
- Establish and enforce controls to access data and systems – such as "acceptable use" policies, mobile device usage, third-party vendor logs, and termination of access for former employees;
- Conduct mandatory and recurring information security training for new and existing employees; and
- Ensure the full engagement of senior management.

OCIE noted that it "will continue to examine for cybersecurity compliance procedures and controls, including testing the implementation of those procedures and controls." Senior SEC officials have warned that cybersecurity remains a priority for the Division of Enforcement as well. In other words, failing to proactively address cybersecurity concerns could lead to exam deficiencies, or worse – attracting the attention of the SEC's Division of Enforcement.

States Are Proactive Too

Firms also should be aware of the recent emergence of comprehensive state cybersecurity compliance requirements. Colorado, for example, recently implemented new rules requiring firms to adopt specific cybersecurity protocols, including conducting annual assessments and using secure email. (See our prior alerts here and here.) And New York enacted specific rules for financial institutions as well. (See our prior alert here.) Other states may well follow. Even if not technically applicable, firms may want to use their local state's requirements as a guide of potentially reasonable procedures.

Unfortunately, cybersecurity risks for regulated entities are not disappearing anytime soon. Thus cybersecurity-related regulatory mandates likely will only increase going forward. To minimize regulatory risks, as well as the significant adverse business and reputational impacts risks that an actual cyber incident might cause, firms and their personnel should proactively and promptly address potential cybersecurity concerns.

For more information, please contact Brian Hoffman (303.295.8043 / bnhoffman@hollandhart.com) and Romain Marshall (801.799.5922 / rcmarshall@hollandhart.com).
