Client Update

SEC Releases Observations from Cybersecurity Examinations

On August 7, 2017, the Office of Compliance Inspections and Examinations ("OCIE") of the Securities and Exchange Commission issued a Risk Alert announcing observations from its second round of cybersecurity examinations of registered broker-dealers, investment advisers, and investment companies.[1] The observations were based on OCIE's examinations of 75 firms since September 2015, pursuant to its "Cybersecurity 2 Initiative"[2] which focused on six areas: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response.

OCIE identified "Issues Observed" (likely providing insight into future enforcement priorities), "Robust Controls" (giving some indication of OCIE's view of best practices), and "Summary of Examination Observations" (lending insight into the current state of the industry). Each is summarized below.

ISSUES OBSERVED

OCIE's guidance called out several areas for attention:

- Policies were not "reasonably tailored" because they provided only "general guidance" to employees, were vague, or failed to articulate procedures to implement the policies;
- Policies failed to reflect actual practices by, for example, calling for annual or continuous reviews of security procedures when in fact those reviews were conducted less frequently;

[1] The full text of the Risk Alert is available through the OCIE webpage, https://www.sec.gov/ocie, or in PDF format at https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

[2] See OCIE *National Exam Program Risk Alert*, OCIE's 2015 Cybersecurity Examination Initiative (September 15, 2015), *available at* http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

- Policies that required all employees to complete cybersecurity training when, in fact, the business did not ensure that training took place and did not take action against employees who failed to attend trainings;
- Contradictory policies;
- Use of outdated technology that is no longer supported by the vendor; and
- Failures to remediate high-risk findings from cybersecurity assessments (*e.g.*, penetration tests or vulnerability scans).

These findings provide a window into likely enforcement priorities. Accordingly, firms should consider reviewing policies – including those regarding cybersecurity training and monitoring – to ensure that they match actual practices. It would also be a good time to take stock of technology that has become obsolete and to consider upgrades. Finally, firms should assess whether they have procedures in place to ensure remediation of vulnerabilities discovered during assessments.

ROBUST CONTROLS

OCIE identified certain practices as "robust," giving some sense of OCIE's view of best practices, including:

- Maintenance of an inventory of data, information, and vendors, including classifications of the risks of each service provider.
- Detailed cybersecurity-related instructions, including policies and procedures relating to penetration tests, security monitoring and system auditing, access rights, and reporting.
- Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities, such as vulnerability scans of core IT infrastructure and patch management policies.
- Established and enforced controls to access data and systems, such as detailed "acceptable use" policies for the firm's networks and equipment, restrictions and controls for mobile devices that connect to the firm's systems, logs of third-party vendors' activities on the firm's networks, and immediate termination of access for terminated employees.
- Mandatory employee training for all employees at on-boarding and periodically thereafter.
- Engaged senior management who vetted and approved the policies and procedures.

SUMMARY OF EXAMINATION OBSERVATIONS

The staff observed that most firms had implemented the following cybersecurity practices, giving some insight into the state of the industry:

- Written policies and procedures addressing cyber-related protection of customer/shareholder records and information.
- Periodic risk assessments of critical systems to identify threats and consequences of cyber incidents.
- Penetration tests and vulnerability scans on critical systems.
- Systems or tools to protect personally identifiable information.
- Regular system maintenance, including the installation of software patches to address security vulnerabilities (although a few firms had not yet installed a significant number of system patches that included critical security updates).
- Policies and procedures addressing cyber-related business continuity planning and Regulation S-P requirements that firms adopt written programs for the protection of customer records and information.
- Policies and procedures addressing cybersecurity and Regulation S-ID requirements that firms adopt written programs to prevent identity theft in connection with certain consumer accounts.
- Response plans for addressing access incidents, denial of service incidents, and authorized intrusions. The staff noted that fewer than two-thirds of advisers and funds maintained such plans.
- Cybersecurity organizational charts and descriptions of cybersecurity roles and responsibilities for the firm's workforce.
- Authority from customers/shareholders to transfer funds to third-party accounts.
- Vendor risk assessments, typically required at the outset of a relationship and in many cases performed at least annually thereafter.

The Risk Alert underscores OCIE's prioritization of cybersecurity risk management and continues a trend of increasing regulatory scrutiny of the details of firms' cybersecurity programs. Leading regulators such as the SEC now expect a comprehensive cybersecurity program of policies, procedures, and technical controls, and they continue to transform best practices into regulatory requirements.

* * *

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Kenneth J. Berman
kjberman@debevoise.com

Luke Dembosky
ldembosy@debevoise.com

Gregory T. Larkin
gtlarkin@debevoise.com

Naeha Prakash
nprakash@debevoise.com

NEW YORK

James Pastore
jjpastore@debevoise.com

Julie Baine Stem
jbstem@debevoise.com