Client Update
SEC Releases Updated Cybersecurity Examination Guidelines

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

David Sarratt
dsarratt@debevoise.com

Lee A. Schneider
lschneider@debevoise.com

Jennifer M. Freeman
jmfreeman@debevoise.com

WASHINGTON, D.C.
Kenneth J. Berman
kjberman@debevoise.com

David A. O'Neil
daoneil@debevoise.com

In 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") conducted examinations of 57 registered broker-dealers and 49 registered investment advisers to assess the adequacy of their cybersecurity compliance and controls. OCIE's Examination Priorities for 2015 included continued cybersecurity examinations of broker-dealers and investment advisors, as well as examinations of transfer agents.

Following up on that priority, on September 15, 2015, OCIE issued a Risk Alert announcing that it will conduct a second round of examinations of registered broker-dealers and investment advisors to assess the registrants' cybersecurity preparedness.[1] OCIE identified six areas on which these examinations will focus:

- governance and risk assessment;
- access rights and controls;
- data loss prevention;
- vendor management;
- training; and
- incident response.

The Risk Alert includes a sample document request (attached here) that is instructive in its breadth, and continues the regulatory trend of focusing on (1) senior-level engagement with cybersecurity; (2) preparation by companies for cyber events, which includes having an incident response plan and testing it; and (3) management of cyber risk related to the use of third-party vendors.

[1] The full text of the Risk Alert is available through the OCIE webpage, http://www.sec.gov/ocie, or in PDF format at http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

Reflecting that focus, OCIE seeks copies of the policies and procedures relating to protection of customer records and information, information about how firms prevent data loss and classify data, and descriptions of how firms manage cybersecurity risks for third-party vendors. The request also seeks copies of incident response plans, patch management practices, board minutes regarding cyber-related risks and documents regarding employee training about cybersecurity.

Whereas in the first round of exams, many of the requests sought to determine merely whether a firm had policies and procedures regarding certain of these topics, this updated sample document request reflects OCIE's expectation that firms will already have in place policies and procedures on these topics. The revised request also reflects an increased focus on employee access rights and access controls, an issue the FTC has recently highlighted in its guidance.

Because the updated sample request reflects what OCIE views as important elements of a firm's cybersecurity program, SEC registrants should review the sample document request closely and address any gaps that a potential examination might reveal in the firm's cybersecurity program. The adequacy of a firm's cybersecurity protections is likely to be a continued focus for OCIE in future exams.

* * *

Please do not hesitate to contact us with any questions.

APPENDIX

This document[1] provides a sample list of information that the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") may review in conducting examinations of registered entities regarding cybersecurity matters. Some of the questions track information outlined in the "Framework for Improving Critical Infrastructure Cybersecurity,"[2] released on February 12, 2014 by the National Institute of Standards and Technology. OCIE has published this document as a resource for registered entities. This document should not be considered all inclusive of the information that OCIE may review or the validation and testing we may perform of firm policies and procedures. Accordingly, OCIE will alter its requests for information it reviews, as well as whether it asks for production of information in advance of an examination or reviews certain information on site, as it considers the specific circumstances presented by each firm's business model, systems, and information technology environment.

Governance and Risk Assessment

- Firm policies and procedures related to the following:

    - Protection of broker-dealer customer and/or investment adviser client (hereinafter "customer") records and information, including those designed to secure customer documents and information, protect against anticipated threats to customer information, and protect against unauthorized access to customer accounts or information; and

    - Patch management practices, including those regarding the prompt installation of critical patches and the documentation evidencing such actions.

- Board minutes and briefing materials, if applicable, regarding: cyber-related risks; cybersecurity incident response planning; actual cybersecurity incidents; and cybersecurity-related matters involving vendors.

- Information regarding the firm's Chief Information Security Officer ("CISO") or equivalent position, and other employees responsible for cybersecurity matters.

- Information regarding the firm's organizational structure, particularly information regarding the positions and departments responsible for cybersecurity-related matters and where they fit within the firm's organization or hierarchy.

[1] The statements and views expressed herein are those of the staff of OCIE. This guidance is not a rule, regulation, or statement of the Commission. The Commission has expressed no view on its contents. This document was prepared by the SEC staff and is not legal advice.

[2] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (February 12, 2014).

- Information regarding the firm's periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business and compliance consequences, if applicable, and any related findings and responsive remediation efforts taken.

- Information regarding the firm's policies related to penetration testing, whether conducted by or on behalf of the firm, and any related findings and responsive remediation efforts taken.

- Information regarding the firm's vulnerability scans and any related findings and responsive remediation efforts taken.

Access Rights and Controls

- Firm policies and procedures regarding access by unauthorized persons to firm network resources and devices and user access restrictions (e.g., access control policy, acceptable use policy, administrative management of systems, and corporate information security policy), including those addressing the following:

  - Establishing employee access rights, including the employee's role or group membership;

  - Updating or terminating access rights based on personnel or system changes; and

  - Any management approval required for changes to access rights or controls.

- Information demonstrating the implementation of firm policies and procedures related to employee access rights and controls, such as the following:

  - Documentation evidencing the tracking of employee access rights, changes to those access rights, and any manager approvals for those changes;

  - Information related to former employees' last date of employment and the date their access to the firm's systems was terminated; and

  - Information related to current employees who have been reassigned by the firm to a new group or function, including their date of reassignment and the date their access to the firm's systems was modified.

- Information related to the systems or applications for which the firm uses multi-factor authentication for employee and customer access as well as documentation evidencing implementation of any related policies and procedures and information on systems or applications for which the firm does not use multi-factor authentication.

- Firm policies and procedures related to log-in attempts, log-in failures, lockouts, and unlocks or resets for perimeter-facing systems and information regarding the process the firm uses to enforce these policies and procedures and to review perimeter-facing systems for failed log-in attempts, deactivation of access, dormant user accounts, and unauthorized log-in attempts.

- Information related to instances in which system users, including employees, customers, and vendors, received entitlements or access to firm data, systems, or reports in contravention of the firm's policies or practices or without required authorization as well as information related to any remediation efforts undertaken in response.

- Firm policies and procedures regarding system notifications to users, including employees and customers, of appropriate usage obligations when logging into the firm's system (e.g., log-on banners, warning messages, or acceptable use notifications) and sample documentation evidencing implementation of these policies and procedures.

- Firm policies and procedures regarding devices used to access the firm's system externally (i.e., firm-issued and personal devices), including those addressing the encryption of such devices and the firm's ability to remotely monitor, track, and deactivate remote devices.

- Information related to customer complaints received by the firm related to customer access, including a description of the resolution of the complaints and any remediation efforts undertaken in response.

- Firm policies and procedures related to verification of the authenticity of customer requests to transfer funds.

- Information related to any reviews of employee access rights and restrictions with respect to job-specific resources within the network and any related documentation.

- Information related to any internal audit conducted by the firm that covered access rights and controls.

Data Loss Prevention

- Firm policies and procedures related to enterprise data loss prevention and information related to the following:

    - Data mapping, with particular emphasis on understanding information ownership and how the firm documents or evidences personally identifiable information ("PII"); and

    - The systems, utilities, and tools used to prevent, detect, and monitor data loss as it relates to PII and access to customer accounts, including a description of the functions and source of these resources.

- Firm policies related to data classification, including: information regarding the types of data classification; the risk level (e.g., low, medium, or high) associated with each data classification; the factors considered when classifying data; and how the factors and risks are considered when the firm makes data classification determinations.

- Firm policies and procedures related to monitoring exfiltration and unauthorized distribution of sensitive information outside of the firm through various distribution channels (e.g., email, physical media, hard copy, or web-based file transfer programs) and any documentation evidencing this monitoring.

Vendor Management

- Firm policies and procedures related to third-party vendors, such as those addressing the following:
  - Due diligence with regard to vendor selection;
  - Contracts, agreements, and the related approval process;
  - Supervision, monitoring, tracking, and access control; and
  - Any risk assessments, risk management, and performance measurements and reports required of vendors.

- Information regarding third-party vendors with access to the firm's network or data, including the services provided and contractual terms related to accessing firm networks or data.

- Information regarding third-party vendors that facilitate the mitigation of cybersecurity risks by means related to access controls, data loss prevention, and management of PII, including a description of the services each vendor provides to the firm and contractual terms included in vendor contracts involving cybersecurity-related services.

- Information regarding written contingency plans the firm has with its vendors concerning, for instance, conflicts of interest, bankruptcy, or other issues that might put the vendor out of business or in financial difficulty.

- Sample documents or notices required of third-party vendors, such as those required prior to any significant changes to the third-party vendors' systems, components, or services that could potentially have security impacts to the firm and the firm's data containing PII.

Training

- Information with respect to training provided by the firm to its employees regarding information security and risks, including the training method (e.g., in person, computer-based learning, or email alerts); dates, topics, and groups of participating employees; and any written guidance or materials provided.

- Information regarding training provided by the firm to third-party vendors or business partners related to information security.

Incident Response

- Firm policies and procedures or the firm's business continuity of operations plan that address mitigation of the effects of a cybersecurity incident and/or recovery from such an incident, including policies regarding cybersecurity incident response and responsibility for losses associated with attacks or intrusions impacting clients.

- Information regarding the firm's process for conducting tests or exercises of its incident response plan, including the frequency of, and reports from, such testing and any responsive remediation efforts taken, if applicable.

- Information regarding system-generated alerts related to data loss of sensitive information or confidential customer records and information, including any related findings and any responsive remediation efforts taken.

- Information regarding incidents of unauthorized internal or external distributions of PII, including the date of the incidents, discovery process, escalation, and any responsive remediation efforts taken.

- Information regarding successful unauthorized internal or external incidents related to access, including the date of the incidents, discovery process, escalation, and any responsive remediation efforts taken.

- Information regarding the amount of actual customer losses associated with cyber incidents, as well as information on the following:

  - The amount of customer losses reimbursed by the firm;

  - Whether the firm had cybersecurity insurance coverage, including the types of incidents the insurance covered;

  - Whether any insurance claims related to cyber events were filed; and

  - The amount of cyber-related losses recovered pursuant to the firm's cybersecurity insurance coverage.