NATIONAL EXAM PROGRAM
RISK ALERT

By the Office of Compliance Inspections and Examinations ("OCIE")[1]

Volume IV, Issue 8 **September 15, 2015**

OCIE's 2015 Cybersecurity Examination Initiative

In this Alert:

Topic: *Cybersecurity Examination Initiative*

Key Takeaways: *OCIE staff will continue its focus on cybersecurity by conducting examinations of registered broker-dealers and investment advisers. The examinations will focus on key topics including governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response. To assist firms in assessing their cybersecurity preparedness, OCIE has included a sample document request in the Appendix to this Risk Alert.*

I. Introduction

In March 2014, the SEC sponsored a Cybersecurity Roundtable where SEC Commissioners and staff, along with industry representatives, underscored the importance of cybersecurity to the integrity of the market system and customer data protection.[2] In April 2014, OCIE published a Risk Alert announcing a series of examinations to identify cybersecurity risks and assess cybersecurity preparedness in the securities industry.[3] In February 2015, OCIE published summary observations of the findings from these examinations, which discussed some of the legal, regulatory, and compliance issues associated with cybersecurity.[4] Given the continued importance of cybersecurity and the positive response from broker-dealers and advisers on OCIE's efforts, OCIE announced a focus on cybersecurity compliance and controls as part of its 2015 Examination Priorities.[5] OCIE is issuing this Risk Alert to provide additional information on the areas of focus for OCIE's second round of cybersecurity examinations, which will involve more testing to assess implementation of firm procedures and controls.

II. Examinations

In light of recent cybersecurity breaches and continuing cybersecurity threats against financial services firms, the Cybersecurity Examination Initiative is designed to build on OCIE's previous examinations in this area and further assess cybersecurity preparedness in the securities industry, including firms' ability to protect broker-dealer customer and investment adviser client

---

1 The views expressed herein are those of the staff of OCIE, in coordination with other staff of the Securities and Exchange Commission ("SEC or Commission"), including the Division of Trading and Markets and the Division of Investment Management. The Commission has expressed no view on the contents of this Risk Alert. This document was prepared by the SEC staff and is not legal advice.

2 SEC, Cybersecurity Roundtable (March 26, 2015).

3 OCIE, NEP Risk Alert, OCIE Cybersecurity Initiative (April 15, 2014).

4 OCIE, NEP Risk Alert, Cybersecurity Examination Sweep Summary (February 3, 2015).

5 OCIE, Examination Priorities for 2015 (January 13, 2015).

(hereinafter referred to as "customer") information.[6] In addition, public reports have identified cybersecurity breaches related to weaknesses in basic controls.[7] As a result, examiners will gather information on cybersecurity-related controls and will also test to assess implementation of certain firm controls. In order to promote better compliance practices and inform the Commission's understanding of cybersecurity preparedness, this Initiative will focus on the following areas:

- **Governance and Risk Assessment:** Examiners may assess whether registrants have cybersecurity governance and risk assessment processes relative to the key areas of focus discussed below. Examiners also may assess whether firms are periodically evaluating cybersecurity risks and whether their controls and risk assessment processes are tailored to their business. Examiners also may review the level of communication to, and involvement of, senior management and boards of directors.

- **Access Rights and Controls:** Firms may be particularly at risk of a data breach from a failure to implement basic controls to prevent unauthorized access to systems or information, such as multifactor authentication or updating access rights based on personnel or system changes. Examiners may review how firms control access to various systems and data via management of user credentials, authentication, and authorization methods. This may include a review of controls associated with remote access, customer logins, passwords, firm protocols to address customer login problems, network segmentation, and tiered access.

- **Data Loss Prevention:** Some data breaches may have resulted from the absence of robust controls in the areas of patch management and system configuration. Examiners may assess how firms monitor the volume of content transferred outside of the firm by its employees or through third parties, such as by email attachments or uploads. Examiners also may assess how firms monitor for potentially unauthorized data transfers and may review how firms verify the authenticity of a customer request to transfer funds.

- **Vendor Management:** Some of the largest data breaches over the last few years may have resulted from the hacking of third party vendor platforms. As a result, examiners may focus on firm practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms. Examiners may assess how vendor relationships are considered as part of the firm's ongoing risk assessment process as well as how the firm determines the appropriate level of due diligence to conduct on a vendor.

- **Training:** Without proper training, employees and vendors may put a firm's data at risk. Some data breaches may result from unintentional employee actions such as a misplaced laptop, accessing a client account through an unsecured internet connection, or opening

---

[6] Among other requirements, Regulation S-P requires financial institutions, including broker-dealers, investment companies, and investment advisers, registered with the Commission to adopt written policies and procedures reasonably designed to insure the security and confidentiality of customer information and records.

[7] *See, e.g.*, Financial Industry Regulatory Authority, Report on Cybersecurity Practices, page 38 (February 2015).

messages or downloading attachments from an unknown source. With proper training, however, employees and vendors can be the firm's first line of defense, such as by alerting firm IT professionals to suspicious activity and understanding and following firm protocols with respect to technology. Examiners may focus on how training is tailored to specific job functions and how training is designed to encourage responsible employee and vendor behavior. Examiners also may review how procedures for responding to cyber incidents under an incident response plan are integrated into regular personnel and vendor training.

- **Incident Response:** Firms generally acknowledge the increased risks related to cybersecurity attacks and potential future breaches. Examiners may assess whether firms have established policies, assigned roles, assessed system vulnerabilities, and developed plans to address possible future events. This includes determining which firm data, assets, and services warrant the most protection to help prevent attacks from causing significant harm.

While these are the primary focus areas for the Cybersecurity Examination Initiative, examiners may select additional areas based on risks identified during the course of the examinations. As part of OCIE's efforts to promote compliance and to share with the industry where it sees cybersecurity-related risks, OCIE is including, as the Appendix to this Risk Alert, a sample request for information and documents to be used in this Initiative.

III. Conclusion

In sharing the key focus areas for the Cybersecurity Examination Initiative and the attached document request, the NEP hopes to encourage registered broker-dealers and investment advisers to reflect upon their own practices, policies, and procedures with respect to cybersecurity.

This Risk Alert is intended to highlight for firms risks and issues that the staff has identified. In addition, this Risk Alert describes factors that firms may consider to (i) assess their supervisory, compliance and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. These factors are not exhaustive, nor will they constitute a safe harbor. Other factors besides those described in this Risk Alert may be appropriate to consider, and some of the factors may not be applicable to a particular firm's business. While some of the factors discussed in this Risk Alert reflect existing regulatory requirements, they are not intended to alter such requirements. Moreover, future changes in laws or regulations may supersede some of the factors or issues raised here. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.

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.