NATIONAL EXAM PROGRAM
RISK ALERT

By the Office of Compliance Inspections and Examinations[1]

Volume IV, Issue 2 **April 15, 2014**

Topic: Cybersecurity Examinations

Key Takeaways: OCIE will be conducting examinations of more than 50 registered broker-dealers and registered investment advisers, focusing on areas related to cybersecurity. In order to empower compliance professionals with questions and tools they can use to assess their respective firms' cybersecurity preparedness, OCIE has included a sample cybersecurity document request in the Appendix to this Risk Alert.

OCIE CYBERSECURITY INITIATIVE

I. Introduction

The U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) previously announced that its 2014 Examination Priorities included a focus on technology, including cybersecurity preparedness.[2] OCIE is issuing this Risk Alert to provide additional information concerning its initiative to assess cybersecurity preparedness in the securities industry.

II. Background

On March 26, 2014, the SEC sponsored a Cybersecurity Roundtable. In opening the Roundtable, Chair Mary Jo White underscored the importance of this area to the integrity of our market system and customer data protection. Chair White also emphasized the "compelling need for stronger partnerships between the government and private sector" to address cyber threats.[3] Commissioner Aguilar, who recommended holding a Cybersecurity Roundtable, emphasized the importance for the Commission to gather information and "consider what additional steps the Commission should take to address cyber-threats."[4]

---

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 Examination Priorities for 2014, *available at*: http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf.

3 Chair Mary Jo White, "Opening Statement at SEC Roundtable on Cybersecurity" (March 26, 2014), *available at*: http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468.

4 Commissioner Luis A. Aguilar, "The Commission's Role in Addressing the Growing Cyber-Threat," Statement at SEC Roundtable on Cybersecurity (March 26, 2014), *available at*: http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184.

III. Examinations

OCIE's cybersecurity initiative is designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats. As part of this initiative, OCIE will conduct examinations of more than 50 registered broker-dealers and registered investment advisers focused on the following: the entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats.

As part of OCIE's efforts to promote compliance and to share with the industry where it sees risk, OCIE is including, as the Appendix to this Risk Alert, a sample request for information and documents used in this initiative.

IV. Conclusion

These examinations will help identify areas where the Commission and the industry can work together to protect investors and our capital markets from cybersecurity threats. The sample document request (see Appendix) is intended to empower compliance professionals in the industry with questions and tools they can use to assess their firms' level of preparedness, regardless of whether they are included in OCIE's examinations.

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

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS
100 F STREET, NE
WASHINGTON, DC 20549

April 15, 2014

This document[1] provides a sample list of requests for information that the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) may use 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 request. Accordingly, OCIE will alter its requests for information as it considers the specific circumstances presented by each firm's particular systems or information technology environment.

Identification of Risks/Cybersecurity Governance

1. For each of the following practices employed by the Firm for management of information security assets, please provide the month and year in which the noted action was last taken; the frequency with which such practices are conducted; the group with responsibility for conducting the practice; and, if not conducted firmwide, the areas that are included within the practice. Please also provide a copy of any relevant policies and procedures.

    - Physical devices and systems within the Firm are inventoried.
    - Software platforms and applications within the Firm are inventoried.
    - Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated.
    - Connections to the Firm's network from external sources are catalogued.
    - Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value.
    - Logging capabilities and practices are assessed for adequacy, appropriate retention, and secure maintenance.

---

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," (Feb. 12, 2014), *available at*: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

2. Please provide a copy of the Firm's written information security policy.

3. Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences. If such assessments are conducted:

    a. Who (business group/title) conducts them, and in what month and year was the most recent assessment completed?

    b. Please describe any findings from the most recent risk assessment that were deemed to be potentially moderate or high risk and have not yet been fully remediated.

4. Please indicate whether the Firm conducts periodic risk assessments to identify physical security threats and vulnerabilities that may bear on cybersecurity. If such assessments are conducted:

    a. Who (business group/title) conducts them, and in what month and year was the most recent assessment completed?

    b. Please describe any findings from the most recent risk assessment that were deemed to be potentially moderate or high risk and have not yet been fully remediated.

5. If cybersecurity roles and responsibilities for the Firm's workforce and managers have been explicitly assigned and communicated, please provide written documentation of these roles and responsibilities. If no written documentation exists, please provide a brief description.

6. Please provide a copy of the Firm's written business continuity of operations plan that addresses mitigation of the effects of a cybersecurity incident and/or recovery from such an incident if one exists.

7. Does the Firm have a Chief Information Security Officer or equivalent position? If so, please identify the person and title. If not, where does principal responsibility for overseeing cybersecurity reside within the Firm?

8. Does the Firm maintain insurance that specifically covers losses and expenses attributable to cybersecurity incidents? If so, please briefly describe the nature of the coverage and indicate whether the Firm has filed any claims, as well as the nature of the resolution of those claims.

Protection of Firm Networks and Information

9. Please identify any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), the Firm has used to model its information security architecture and processes.

10. Please indicate which of the following practices and controls regarding the protection of its networks and information are utilized by the Firm, and provide any relevant policies and procedures for each item.

- The Firm provides written guidance and periodic training to employees concerning information security risks and responsibilities. If the Firm provides such guidance and/or training, please provide a copy of any related written materials (*e.g.*, presentations) and identify the dates, topics, and which groups of employees participated in each training event conducted since January 1, 2013.

- The Firm maintains controls to prevent unauthorized escalation of user privileges and lateral movement among network resources. If so, please describe the controls, unless fully described within policies and procedures.

- The Firm restricts users to those network resources necessary for their business functions. If so, please describe those controls, unless fully described within policies and procedures.

- The Firm maintains an environment for testing and development of software and applications that is separate from its business environment.

- The Firm maintains a baseline configuration of hardware and software, and users are prevented from altering that environment without authorization and an assessment of security implications.

- The Firm has a process to manage IT assets through removal, transfers, and disposition.

- The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities.

- The Firm's information security policy and training address removable and mobile media.

- The Firm maintains controls to secure removable and portable media against malware and data leakage. If so, please briefly describe these controls.

- The Firm maintains protection against Distributed Denial of Service (DDoS) attacks for critical internet-facing IP addresses. If so, please describe the internet functions protected and who provides this protection.

- The Firm maintains a written data destruction policy.

- The Firm maintains a written cybersecurity incident response policy. If so, please provide a copy of the policy and indicate the year in which it was most recently updated. Please also indicate whether the Firm conducts tests or exercises to assess its incident response policy, and if so, when and by whom the last such test or assessment was conducted.

- The Firm periodically tests the functionality of its backup system. If so, please provide the month and year in which the backup system was most recently tested.

11. Please indicate whether the Firm makes use of encryption. If so, what categories of data, communications, and devices are encrypted and under what circumstances?

12. Please indicate whether the Firm conducts periodic audits of compliance with its information security policies. If so, in what month and year was the most recent such audit completed, and by whom was it conducted?

Risks Associated With Remote Customer Access and Funds Transfer Requests

13. Please indicate whether the Firm provides customers with on-line account access. If so, please provide the following information:

    a. The name of any third party or parties that manage the service.

    b. The functionality for customers on the platform (*e.g.*, balance inquiries, address and contact information changes, beneficiary changes, transfers among the customer's accounts, withdrawals or other external transfers of funds).

    c. How customers are authenticated for on-line account access and transactions.

    d. Any software or other practice employed for detecting anomalous transaction requests that may be the result of compromised customer account access.

    e. A description of any security measures used to protect customer PINs stored on the sites.

    f. Any information given to customers about reducing cybersecurity risks in conducting transactions/business with the Firm.

14. Please provide a copy of the Firm's procedures for verifying the authenticity of email requests seeking to transfer customer funds. If no written procedures exist, please describe the process.

15. Please provide a copy of any Firm policies for addressing responsibility for losses associated with attacks or intrusions impacting customers.

    a. Does the Firm offer its customers a security guarantee to protect them against hacking of their accounts? If so, please provide a copy of the guarantee if one exists and a brief description.

Risks Associated With Vendors and Other Third Parties

16. If the Firm conducts or requires cybersecurity risk assessments of vendors and business partners with access to the Firm's networks, customer data, or other sensitive information, or due to the cybersecurity risk of the outsourced function, please describe who conducts this assessment, when it is required, and how it is conducted. If a questionnaire is used, please provide a copy. If assessments by independent entities are required, please describe any standards established for such assessments.

17. If the Firm regularly incorporates requirements relating to cybersecurity risk into its contracts with vendors and business partners, please describe these requirements and the circumstances in which they are incorporated. Please provide a sample copy.

18. Please provide a copy of policies and procedures and any training materials related to information security procedures and responsibilities for trainings conducted since January 2013 for vendors and business partners authorized to access its network.

19. If the Firm assesses the segregation of sensitive network resources from resources accessible to third parties, who (business group/title) performs this assessment, and provide a copy of any relevant policies and procedures?

20. If vendors, business partners, or other third parties may conduct remote maintenance of the Firm's networks and devices, describe any approval process, logging process, or controls to prevent unauthorized access, and provide a copy of any relevant policies and procedures.

Detection of Unauthorized Activity

21. For each of the following practices employed by the Firm to assist in detecting unauthorized activity on its networks and devices, please briefly explain how and by whom (title, department and job function) the practice is carried out.

- Identifying and assigning specific responsibilities, by job function, for detecting and reporting suspected unauthorized activity.
- Maintaining baseline information about expected events on the Firm's network.
- Aggregating and correlating event data from multiple sources.
- Establishing written incident alert thresholds.
- Monitoring the Firm's network environment to detect potential cybersecurity events.
- Monitoring the Firm's physical environment to detect potential cybersecurity events.
- Using software to detect malicious code on Firm networks and mobile devices.
- Monitoring the activity of third party service providers with access to the Firm's networks.
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm's networks.
- Evaluating remotely-initiated requests for transfers of customer assets to identify anomalous and potentially fraudulent requests.

- Using data loss prevention software.

- Conducting penetration tests and vulnerability scans. If so, please identify the month and year of the most recent penetration test and recent vulnerability scan, whether they were conducted by Firm employees or third parties, and describe any findings from the most recent risk test and/or assessment that were deemed to be potentially moderate or high risk but have not yet been addressed.

- Testing the reliability of event detection processes. If so, please identify the month and year of the most recent test.

- Using the analysis of events to improve the Firm's defensive measures and policies.

Other

22. Did the Firm update its written supervisory procedures to reflect the Identity Theft Red Flags Rules, which became effective in 2013 (17 CFR § 248—Subpart C—Regulation S-ID)?

    a. If not, why?

23. How does the Firm identify relevant best practices regarding cybersecurity for its business model?

24. **Since January 1, 2013**, has your Firm experienced any of the following types of events? If so, please provide a brief summary for each category listed below, identifying the number of such incidents (approximations are acceptable when precise numbers are not readily available) and describing their significance and any effects on the Firm, its customers, and its vendors or affiliates. If the response to any one item includes more than 10 incidents, the respondent may note the number of incidents and describe incidents that resulted in losses of more than $5,000, the unauthorized access to customer information, or the unavailability of a Firm service for more than 10 minutes. The record or description should, at a minimum, include: the extent to which losses were incurred, customer information accessed, and Firm services impacted; the date of the incident; the date the incident was discovered and the remediation for such incident.

    - Malware was detected on one or more Firm devices. Please identify or describe the malware.

    - Access to a Firm web site or network resource was blocked or impaired by a denial of service attack. Please identify the service affected, and the nature and length of the impairment.

    - The availability of a critical Firm web or network resource was impaired by a software or hardware malfunction. Please identify the service affected, the nature and length of the impairment, and the cause.

    - The Firm's network was breached by an unauthorized user. Please describe the nature, duration, and consequences of the breach, how the Firm learned of it, and how it was remediated.

- The compromise of a customer's or vendor's computer used to remotely access the Firm's network resulted in fraudulent activity, such as efforts to fraudulently transfer funds from a customer account or the submission of fraudulent payment requests purportedly on behalf of a vendor.

- The Firm received fraudulent emails, purportedly from customers, seeking to direct transfers of customer funds or securities.

- The Firm was the subject of an extortion attempt by an individual or group threatening to impair access to or damage the Firm's data, devices, network, or web services.

- An employee or other authorized user of the Firm's network engaged in misconduct resulting in the misappropriation of funds, securities, sensitive customer or Firm information, or damage to the Firm's network or data.

25. **Since January 1, 2013**, if not otherwise reported above, did the Firm, either directly or as a result of an incident involving a vendor, experience the theft, loss, unauthorized exposure, or unauthorized use of or access to customer information? Please respond affirmatively even if such an incident resulted from an accident or negligence, rather than deliberate wrongdoing. If so, please provide a brief summary of each incident or a record describing each incident.

26. For each event identified in response to Questions 24 and 25 above, please indicate whether it was reported to the following:

    - Law enforcement (please identify the entity)

    - FinCEN (through the filing of a Suspicious Activity Report)

    - FINRA

    - A state or federal regulatory agency (please identity the agency and explain the manner of reporting)

    - An industry or public-private organization facilitating the exchange of information about cybersecurity incidents and risks

27. What does the Firm presently consider to be its three most serious cybersecurity risks, and why?

28. Please feel free to provide any other information you believe would be helpful to the Securities and Exchange Commission in evaluating the cybersecurity posture of the Firm or the securities industry.