NATIONAL EXAM PROGRAM
RISK ALERT

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

Volume VI, Issue 5 **August 7, 2017**

This Risk Alert provides a summary of observations from OCIE's examinations of registered broker-dealers, investment advisers, and investment companies conducted pursuant to the Cybersecurity Examination Initiative announced on September 15, 2015.

OBSERVATIONS FROM CYBERSECURITY EXAMINATIONS

I. Introduction

In OCIE's Cybersecurity 2 Initiative, National Examination Program staff examined 75 firms, including broker-dealers, investment advisers, and investment companies ("funds") registered with the SEC to assess industry practices and legal and compliance issues associated with cybersecurity preparedness.[2] The Cybersecurity 2 Initiative built upon prior cybersecurity examinations, particularly OCIE's 2014 Cybersecurity 1 Initiative.[3] However, the Cybersecurity 2 Initiative examinations involved more validation and testing of procedures and controls surrounding cybersecurity preparedness than was previously performed.

The examinations focused on the firms' written policies and procedures regarding cybersecurity, including validating and testing that such policies and procedures were implemented and followed. In addition, the staff sought to better understand how firms managed their cybersecurity preparedness by focusing on the following areas: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response.

In general, the staff observed increased cybersecurity preparedness since our 2014 Cybersecurity 1 Initiative. However, the staff also observed areas where compliance and oversight could be improved. This Risk Alert provides a summary of the staff's observations from the Cybersecurity 2 Initiative

---

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"). 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 *See* OCIE, *Examination Priorities for 2015* (January 13, 2015) and *National Exam Program Risk Alert, OCIE's 2015 Cybersecurity Examination Initiative* (September 15, 2015). A few of the staff's observations discussed herein were previously discussed in a recent *National Exam Program Risk Alert, Cybersecurity: Ransomware Alert* (May 17, 2017).

3 *See* OCIE, *OCIE Cybersecurity Initiative* (April 15, 2014) and *National Exam Program Risk Alert, Cybersecurity Examination Sweep Summary* (February 3, 2015). The staff examined a different population of firms in the Cybersecurity 2 Initiative than those that were examined in the Cybersecurity 1 Initiative.

examinations and highlights certain issues observed as well as certain policies and procedures that the staff believes may be effective.[4]

II. Summary of Examination Observations

Among the 75 firms examined, the staff noted an overall improvement in firms' awareness of cyber-related risks and the implementation of certain cybersecurity practices since the Cybersecurity 1 Initiative. Most notably, all broker-dealers, all funds, and nearly all advisers examined maintained cybersecurity-related written policies and procedures addressing the protection of customer/shareholder records and information. This contrasts with the staff's observations in the Cybersecurity 1 Initiative, in which comparatively fewer broker-dealers and advisers had adopted this type of written policies and procedures.

In the examinations, the staff observed:

- Nearly all broker-dealers and the vast majority of advisers and funds conducted periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities, and the potential business consequences of a cyber incident.

- Nearly all broker-dealers and almost half of the advisers and funds conducted penetration tests and vulnerability scans on systems that the firms considered to be critical, although a number of firms did not appear to fully remediate some of the high risk observations that they discovered from these tests and scans during the review period.

- All firms utilized some form of system, utility, or tool to prevent, detect, and monitor data loss as it relates to personally identifiable information.

- All broker-dealers and nearly all advisers and funds had a process in place for ensuring regular system maintenance, including the installation of software patches to address security vulnerabilities. However, the staff observed that a few of the firms had a significant number of system patches that, according to the firms, included critical security updates that had not yet been installed.

- Information protection programs at the firms typically included relevant cyber-related topics, such as:

    - *Policies and procedures*. Nearly all firms' policies and procedures addressed cyber-related business continuity planning and Regulation S-P.[5] In addition, nearly all broker-dealers and

---

[4] The examinations were conducted between September 2015 and June 2016 and generally covered the review period October 1, 2014 through September 30, 2015.

[5] *See* 17 C.F.R. Part 248, Subpart A—*Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information*. *See also Disposal of Consumer Report Information*, Securities Exchange Act of 1934 ("Exchange Act") Release No. 50781, Investment Advisers Act of 1940 ("Advisers Act") Release No. 2332, Investment Company Act of 1940 ("Investment Company Act") Release No. 26685 (December 2, 2004), 69 Fed. Reg. 71321 (December 8, 2004) and *Privacy of Consumer Financial Information (Regulation S-P)*, Exchange Act Release No. 42974, Investment Company Act Release No. 24543, Advisers Act Release No. 1883 (June 22, 2000), 65 Fed. Reg. 40334 (June 29, 2000).

most advisers and funds had specific cybersecurity and Regulation S-ID[6] policies and procedures.

- *Response plans.* Nearly all of the firms had plans for addressing access incidents. In addition, the vast majority of firms had plans for denial of service incidents and unauthorized intrusions. However, while the vast majority of broker-dealers maintained plans for data breach incidents and most had plans for notifying customers of material events, less than two-thirds of the advisers and funds appeared to maintain such plans.

- All broker-dealers and a large majority of advisers and funds maintained cybersecurity organizational charts and/or identified and described cybersecurity roles and responsibilities for the firms' workforce.

- The vast majority of broker-dealers and nearly two-thirds of the advisers and funds had authority from customers/shareholders to transfer funds to third party accounts.

  - Some of the broker-dealers did not appear to memorialize their processes into written supervisory procedures. Rather, these broker-dealers appeared to have informal practices for verifying customers' identities in order to proceed with requests to transfer funds.

  - All of the advisers and funds maintained policies, procedures, and standards related to verifying the authenticity of a customer/shareholder who was requesting to transfer funds.

- Almost all firms either conducted vendor risk assessments or required that vendors provide the firms with risk management and performance reports (i.e., internal and/or external audit reports) and security reviews or certification reports. While vendor risk assessments are typically conducted at the outset of a relationship, over half of the firms also required updating such risk assessments on at least an annual basis.

III. Issues Observed

The staff observed one or more issues in the vast majority of the Cybersecurity 2 Initiative examinations. Highlighted below are issues the staff believes firms would benefit from considering in order to assess and improve their policies, procedures, and practices.

- While, as noted above, all broker-dealers and funds, and nearly all advisers maintained written policies and procedures addressing cyber-related protection of customer/shareholder records and information, a majority of the firms' information protection policies and procedures appeared to have issues. Examples included:

  - *Policies and procedures were not reasonably tailored* because they provided employees with only general guidance, identified limited examples of safeguards for employees to consider, were very narrowly scoped, or were vague, as they did not articulate procedures for implementing the policies.

---

[6] *See* 17 C.F.R. Part 248, Subpart C—*Regulation S–ID: Identity Theft Red Flags*. *See also Identity Theft Red Flags Rules*, Exchange Act Release No. 69359, Advisers Act Release No. 3582, Investment Company Act Release No. 30456 (April 10, 2013), 78 Fed. Reg. 23637 (April 19, 2013).

- *Firms did not appear to adhere to or enforce policies and procedures, or the policies and procedures did not reflect the firms' actual practices,* such as when the policies:
    - Required annual customer protection reviews; however, in practice, they were conducted less frequently.
    - Required ongoing reviews to determine whether supplemental security protocols were appropriate; however, such reviews were performed only annually, or not at all.
    - Created contradictory or confusing instructions for employees, such as policies regarding remote customer access that appeared to be inconsistent with those for investor fund transfers, making it unclear to employees whether certain activity was permissible.
    - Required all employees to complete cybersecurity awareness training; however, firms did not appear to ensure this occurred and take action concerning employees who did not complete the required training.

- The staff also observed Regulation S-P-related issues among firms that did not appear to adequately conduct system maintenance, such as the installation of software patches to address security vulnerabilities and other operational safeguards to protect customer records and information. Examples included:
    - *Stale Risk Assessments*. Using outdated operating systems that were no longer supported by security patches.
    - *Lack of Remediation Efforts*. High-risk findings from penetration tests or vulnerability scans that did not appear to be fully remediated in a timely manner.

IV. Elements of Robust Policies and Procedures[7]

During these examinations, the staff observed several elements that were included in the policies and procedures of firms that the staff believes had implemented robust controls. Firms may wish to consider the following elements as they could be useful in the implementation of cybersecurity-related policies and procedures.[8]

- *Maintenance of an inventory of data, information, and vendors*. Policies and procedures included a complete inventory of data and information, along with classifications of the risks,

---

[7] This is not intended to be a comprehensive list of the elements of robust cybersecurity policies and procedures. The adequacy of supervisory, compliance, and other risk management policies and procedures can be determined only with reference to the profile of each specific firm and other facts and circumstances.

[8] Firms may also wish to consider the guidance and information issued by the SEC's Division of Investment Management and the cybersecurity issues discussed in Commission orders in settled enforcement proceedings. *See, e.g.*, *IM Guidance Update: Cybersecurity Guidance* (April 2015), *In re Morgan Stanley Smith Barney LLC*, Exchange Act Release No. 78021, Advisers Act Release No. 4415 (June 8, 2016), *In re R.T. Jones Capital Equities Management Inc.*, Advisers Act Release No. 4204 (September 22, 2015), and *In re Craig Scott Capital LLC*, Exchange Act Release No. 77595 (April 12, 2016).

vulnerabilities, data, business consequences, and information regarding each service provider and vendor, if applicable.

- *Detailed cybersecurity-related instructions*. Examples included:

  - Penetration tests – policies and procedures included specific information to review the effectiveness of security solutions.

  - Security monitoring and system auditing – policies and procedures regarding the firm's information security framework included details related to the appropriate testing methodologies.

  - Access rights – requests for access were tracked, and policies and procedures specifically addressed modification of access rights, such as for employee on-boarding, changing positions or responsibilities, or terminating employment.

  - Reporting – policies and procedures specified actions to undertake, including who to contact, if sensitive information was lost, stolen, or unintentionally disclosed/misdirected.

- *Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities*. Examples included:

  - Vulnerability scans of core IT infrastructure were required to aid in identifying potential weaknesses in a firm's key systems, with prioritized action items for any concerns identified.

  - Patch management policies that included, among other things, the beta testing of a patch with a small number of users and servers before deploying it across the firm, an analysis of the problem the patch was designed to fix, the potential risk in applying the patch, and the method to use in applying the patch.

- *Established and enforced controls to access data and systems*. For example, the firms:

  - Implemented detailed "acceptable use" policies that specified employees' obligations when using the firm's networks and equipment.

  - Required and enforced restrictions and controls for mobile devices that connected to the firms' systems, such as passwords and software that encrypted communications.

  - Required third-party vendors to periodically provide logs of their activity on the firms' networks.

  - Required immediate termination of access for terminated employees and very prompt (typically same day) termination of access for employees that left voluntarily.

- *Mandatory employee training.* Information security training was mandatory for all employees at on-boarding and periodically thereafter, and firms instituted policies and procedures to ensure that employees completed the mandatory training.

- *Engaged senior management.* The policies and procedures were vetted and approved by senior management.

V. Conclusion

Cybersecurity remains one of the top compliance risks for financial firms.[9] As noted in OCIE's 2017 priorities, OCIE will continue to examine for cybersecurity compliance procedures and controls, including testing the implementation of those procedures and controls at firms.[10]

This Risk Alert is intended to highlight for firms the risks and issues that the staff identified during examinations of broker-dealers, investment advisers, and investment companies regarding cybersecurity preparedness. In addition, this Risk Alert describes factors that firms may consider to (1) assess their supervisory, compliance and/or other risk management systems related to cybersecurity risks, and (2) 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. Factors other than 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 herein. 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.

---

[9] *See, e.g.*, Investment Adviser Association, ACA Compliance Group, and OMAM, *2016 Investment Management Compliance Testing Survey* (June 23, 2016), which synthesizes 730 adviser compliance professionals' responses to 94 compliance-related questions. Q94: 88% of advisers view cybersecurity, privacy, and identity theft as the hottest compliance topic for 2016.

[10] OCIE, *Examination Priorities for 2017* (January 12, 2017).