August 30, 2017

Skadden

# Investment Management Alert


**Contacts**

**Anastasia T. Rockas**
Partner / New York
212.735.2987
anastasia.rockas@skadden.com

**Stuart D. Levi**
Partner / New York
212.735.2750
stuart.levi@skadden.com

**Jessica N. Cohen**
Counsel / New York
212.735.2793
jessica.cohen@skadden.com





Four Times Square
New York, NY 10036
212.735.3000


## OCIE Releases Results of Cybersecurity Examination Initiative

On August 7, 2017, the Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission (SEC) released a summary of its observations (the report) from cybersecurity examinations of 75 registered broker-dealers, investment advisers and investment companies that it conducted pursuant to the Cybersecurity Examination Initiative it announced on September 15, 2015 (the initiative).[1] The initiative's examinations focused on written policies and procedures regarding cybersecurity, with an increased focus on validating and testing that such policies and procedures were implemented and followed as compared to past reviews.

### Background

On September 15, 2015, the SEC issued a risk alert release announcing OCIE's initiative,[2] under which it would undertake to examine registered broker-dealers and investment advisers' cybersecurity preparedness in light of recent breaches and continuing threats against financial services firms. The initiative was designed to build on OCIE's prior cybersecurity examinations conducted in 2014 and would review different firms than those from the prior initiative.

### Key Findings

Overall, OCIE observed improvements in cybersecurity preparedness since its 2014 initiative, but also noted some areas for improvement and concern, which included:

- **Policies and procedures that were not sufficiently detailed.** Some 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 omitted specific procedures for implementing policies.
- **Inconsistent enforcement of policies.** A number of firms did not enforce their own policies and procedures, or in some cases the written policies and procedures did not reflect the firms' actual practices. For example, written policies may require annual customer protection reviews, ongoing reviews of security protocols or completion of cybersecurity training, but, in practice, these reviews or procedures may be occurring less frequently than specified or not at all.

[1] The full text of the report is available here.

[2] OCIE, NEP Risk Alert, "OCIE's 2015 Cybersecurity Initiative" (September 15, 2015). A prior Skadden mailing regarding the initiative is available here.

- **Inadequate system maintenance leading to violations of Regulation S-P.** The SEC's Regulation S-P requires investment advisers to adopt policies and procedures that address technical and physical safeguards to protect customer records and information. However, OCIE staff found Regulation S-P violations among firms that did not adequately conduct system maintenance, such as installing software patches to address security vulnerabilities or implementing additional operational safeguards.

### OCIE Recommendations

OCIE staff also outlined a number of firms' practices and policies that should serve as best practices, including:

- **Maintaining an inventory of data, information and vendors.** Policies and procedures should include a complete inventory of data and information, with classifications of the risks, vulnerabilities, data, business consequences and information regarding each service provider and vendor.
- **Drafting detailed cybersecurity-related instructions.** In particular, details should be included for penetration tests, security monitoring and system auditing, access rights and reporting requirements.
- **Maintaining prescriptive schedules and processes for testing data integrity and vulnerabilities.** For example, patch management policies should include beta testing a patch with a small number of users and servers before deploying it firmwide.
- **Establishing and enforcing controls to access data and systems.** This includes implementing detailed "acceptable use" policies, requiring restrictions and controls for mobile devices, requiring third-party vendors to periodically log their activities on the firms' networks and immediately ceasing access of terminated employees.
- **Requiring mandatory employee training.** Information security training should be mandatory for all employees at time of hire and periodically thereafter, and firms should institute policies and procedures to ensure that employees complete the mandatory training.
- **Engaged senior management.** The policies and procedures should be vetted and approved by senior management.

### Ransomware Attack Prevention

Additionally, on May 17, 2017, OCIE issued a cybersecurity risk alert (the ransomware alert) regarding the widespread ransomware attack known as WannaCry.[3] Similar to other ransomware attacks, WannaCry, infected computers with malicious software that encrypted computer users' files and demanded payment to restore access to the locked files. In the ransomware alert, broker-dealers and investment management companies were encouraged to (1) review the alert published by the United States Department of Homeland Security's Computer Emergency Readiness Team[4] and (2) evaluate whether applicable Microsoft patches for Windows XP, Windows 8 and Windows Server 2003 operating systems were properly and timely installed. The ransomware alert cautioned that smaller registrants may be at greater risk. It also pointed to observations from the initiative and outlined measures that firms should implement to mitigate the impact of ransomware attacks, including conducting: (1) periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities and potential business consequences, (2) penetration tests and vulnerability scans on systems that the firms considered to be critical and (3) regular system maintenance, including on software patches to address security vulnerabilities.

### Conclusion

As noted in OCIE's "Examination Priorities for 2017,"[5] cybersecurity compliance and procedures remain a top priority. In light of OCIE's continued interest in promoting the Cybersecurity Examination Initiative, it would be prudent for broker-dealers, investment advisers and investment companies to review their cybersecurity policies and preparedness and develop a rapid response plan.

[3] OCIE's "Cybersecurity: Ransomware Alert" is available here.

[4] The United States Department of Homeland Security's Computer Emergency Readiness Team alert is available here.

[5] OCIE's "Examination Priorities for 2017" are available here.