Published on *The National Law Review* https://natlawreview.com

SEC Observations from Recent Cybersecurity Examinations Identify Best Practices

Article By:

Mark L. Krotoski

Christine M. Lombardo

Martin Hirschprung

The SEC continues to focus on cybersecurity as an area of concern within the investment management industry.

On August 7, the US Securities and Exchange Commission's (SEC's) Office of Compliance Inspections and Examinations (OCIE) released a Risk Alert summarizing its observations from a recent cybersecurity-related examination of 75 firms—including broker-dealers, investment advisers, and investment companies ("funds") registered with the SEC.

The SEC staff has made it clear that cybersecurity remains a high priority and is likely to be an area of continued scrutiny with the potential for enforcement actions. During a recent interview,[1] the SEC's co-directors of Enforcement, Stephanie Avakian and Steven Peikin, stated their belief that "[t]he greatest threat to our markets right now is the cyber threat." This pronouncement follows on the heels of OCIE's identification of cybersecurity as one of its examination priorities for 2017,[2] OCIE's release of a Risk Alert on the "WannaCry" ransomware virus,[3] and several significant Regulation S-P enforcement actions involving firms that failed to adequately protect customer information.[4]

This LawFlash details OCIE's observations from its recent cybersecurity-related examination that were discussed in its Risk Alert.

OCIE's Examination Identifies Common Issues

OCIE staff observed common issues in a majority of the firms and funds subject to examination. These common issues include the following:

- Failure to reasonably tailor policies and procedures. Specifically, the examination found issues with policies and procedures that
    - incorporated only general guidance;

- identified limited examples of safeguards for employees to consider; and
- did not articulate specific procedures to implement policies.

- Failure to adhere to or enforce policies and procedures. In some cases, policies and procedures were confusing or did not reflect a firm's actual practices, including in the following areas:
  - Annual customer protection reviews not actually conducted on an annual basis
  - Policies providing for ongoing reviews to determine whether supplemental security protocols were appropriate performed only annually, or not at all
  - Policies and procedures creating contradictory or confusing instructions for employees[5]
  - Firms not appearing to adequately ensure that cybersecurity awareness training was provided and/or failing to take action where employees did not complete required cybersecurity training

- Regulation S-P issues among firms that did not appear to adequately conduct system maintenance. Because Regulation S-P was enacted to safeguard the privacy of customer information, OCIE observed that issues arose where firms failed to install software patches to address security vulnerabilities and other operational safeguards to protect customer records and information.

- Failure to fully remediate some of the high-risk observations that firms discovered when they conducted penetration tests and vulnerability scans.

Cyber Best Practices and Other Observations

OCIE identified elements of what it viewed as "robust" cybersecurity policies and procedures from its examinations. Such elements should be considered as best practices and instructive for broker-dealers, investment advisers, and funds in implementing, assessing, and/or enhancing existing cybersecurity-related policies and procedures. Such elements are as follows:

- Maintenance of data, information, and vendor inventory, including risk classifications
- Detailed cybersecurity-related instructions, including instructions related to penetration tests, access rights, and reporting guidelines for lost, stolen, or unintentionally disclosed sensitive information
- Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities, including patch management policies
- Access controls for data and systems
- Mandatory employee training upon onboarding and periodically thereafter

- Engaged senior management

OCIE staff noted an overall improvement in firms' awareness of cyber-related risks and the implementation of certain cybersecurity practices since its previous Cybersecurity 1 Initiative.[6] Most notably, all broker-dealers, all funds, and nearly all investment advisers in the more recent examinations maintain written policies and procedures related to cybersecurity that address the protection of customer/shareholder records and information. This finding is in contrast to the Cybersecurity 1 Initiative, where OCIE found that comparatively fewer broker-dealers and investment advisers had adopted this type of written policies and procedures.

OCIE staff also noted the following:

- Nearly all broker-dealers and many investment advisers and funds conducted periodic risk assessments, penetration tests, and vulnerability scans.
- All broker-dealers and nearly all investment advisers and funds had a process in place for ensuring regular system maintenance.
- 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 a majority of investment advisers and funds maintained cybersecurity organizational charts and/or identified and described cybersecurity roles and responsibilities for the firms' workforces.
- 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.
- Information protection programs at the firms typically included relevant cyber-related policies and procedures as well as incident response plans.

Key Takeaways

SEC-registered broker-dealers, investment advisers, and funds should evaluate their policies and procedures to determine whether there are gaps or areas that could be improved based on OCIE's articulation of best practices. Firms and funds should further evaluate their policies and procedures to ensure that they reflect actual practices and are reasonably tailored to the particular firm's business. As OCIE notes, effective cybersecurity requires a *tailored and risk-based approach* to safeguard information and systems.[7]

---

[1] Sarah Lynch, *Exclusive: New SEC Enforcement Chiefs See Cyber Crime as Biggest Market Threat*, Reuters.com (Jun. 8, 2017).

[2] OCIE, Examination Priorities for 2017 (Jan. 12, 2017).

[3] National Exam Program Risk Alert, Cybersecurity: Ransomware Alert (May 17, 2017).

[4] *In re Morgan Stanley Smith Barney LLC*, Exchange Act Release No. 78021, Advisers Act Release No. 4415 (Jun. 8, 2016); *In re R.T. Jones Capital*

Equities Management Inc., Advisers Act Release No. 4204 (Sept. 22, 2015); and *In re Craig Scott Capital LLC*, Exchange Act Release No. 77595 (Apr. 12, 2016).

[5] OCIE provides an example of confusing 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 based on the policies.

[6] *See, e.g.,* OCIE Cybersecurity Initiative (Apr. 15, 2014); *see also* National Exam Program Risk Alert, Cybersecurity Examination Sweep Summary (Feb. 3, 2015).

[7] For example, the National Institute of Standards and Technology Cybersecurity Framework 1.0 (Feb. 12, 2014) provides a useful flexible approach to assess and manage cybersecurity risk.

National Law Review, Volume VII, Number 227