Blogs
August 15, 2017
Asset Management ADVocate

SEC Offers More Guidance on Cybersecurity Best Practices and Pitfalls - Part 1 of 2

On August 7, 2017, the SEC's Office of Compliance Inspections and Examinations ("OCIE") released a Risk Alert summarizing its conclusions from a year-long review of the cybersecurity practices of a 75 firms — including broker-dealers, investment advisers and investment companies. The sweep, OCIE's Cybersecurity 2 Initiative, ran from September 2015 to June 2016 and covered the review period from October 2014 through September 2015. It follows OCIE's 2014 Cybersecurity 1 Initiative, during which the staff examined a different group of firms from January 2013 to June 2014. The Risk Alert that followed the first sweep was released in early 2015. The focus of OCIE's second sweep was asset management firms' written cybersecurity policies and procedures and, critically, their implementation. While the Risk Alert acknowledges that cybersecurity preparedness has improved across the industry since the first sweep exam, it emphasizes that significant deficiencies persist. The Risk Alert identifies common elements of policies and procedures that the staff regards as robust controls. The Risk Alert also stresses that, going forward, OCIE will increase its review of firms' implementation of appropriately-tailored policies; merely having well?drafted policies "on the books" but not applied will not suffice.

Recurring Cybersecurity Issues

The Risk Alert discusses several areas of widespread deficiency that the OCIE staff believes can serve as guideposts for firms to improve their policies, procedures and practices. While nearly all of the 75 firms evaluated in the Cybersecurity 2 sweep had written policies and procedures addressing cyber-related business continuity planning and Regulation S-P, and most advisers and funds had specific cybersecurity and Regulation S-ID policies and procedures, a majority of firms had weaknesses, including that:

- their policies "were not reasonably tailored," providing only vague, general guidance, and did not correspond to specific procedures for employees to follow in implementing the policies;
- they failed to adhere to, or in practice did not actually follow, key established policies and procedures, including:
    - mandatory annual customer protection reviews;
    - annual and ongoing reviews of security protocol appropriateness;
    - required employee cybersecurity training and disciplinary provisions for employees who disregarded such training; and
- their policies generally did not provide clear and non-contradictory instructions, and instead were often inconsistent, such as with respect to remote customer access and investor fund transfer restrictions.

Additionally, the Risk Alert discusses concerns regarding firms:

- using legacy operating systems that do not support new security patches;
- failing to timely install software patches and other operational safeguards for protecting customer information;
- conducting penetration tests but failing to fully remediate high-risk findings from those tests in a timely manner; and
- failing to appropriately adhere to Regulation S-P.

Elements of Effective Policies and Procedures

The Risk Alert identifies the elements of policies and procedures that the OCIE staff believes should be part of a "robust" set of cybersecurity controls. The guidance offered in the Risk Alert is quite specific, detailing the major elements of cybersecurity policies and procedures firms should consider to improve their programs. The critical policy elements that the OCIE staff favorably identified during the Cybersecurity 2 sweep exam include the following.

Maintenance of an inventory of data, information, and vendors/service providers. Well-developed policies and procedures include complete inventories of data residing on a firm's networks and classifications of the risks, vulnerabilities, data, business consequences and information regarding each third-party vendor/service provider used by the firm.

Penetration Tests. Policies and procedures should contain specific information necessary to review the effectiveness of the testing and security solutions.

Security Monitoring and System Auditing. Policies and procedures concerning a firm's information security framework should include details related to appropriate testing methodologies.

Access Rights. Procedures should track requests for network access and include policies specifically address the modification of user access rights, including for employee hiring and termination and the changing of employee positions/responsibilities.

Reporting. Procedures should contain specific action plans, including the names of individuals to contact if sensitive information is lost, stolen, unintentionally disclosed or otherwise compromised.

Part 2 of this blog discusses additional cybersecurity program elements identified in the Risk Alert and suggests key takeaways from the guidance.

Explore more in

Investment Management
Blog series

Asset Management ADVocate

The Asset Management ADVocate provides unique analysis and insight into legal developments affecting asset managers in the United States.

View the blog