OCIE Lessons From Cybersecurity 2 Initiative

CYBERSECURITY AND PRIVACY | FINANCIAL SERVICES REGULATORY | LIFE, ANNUITY, AND RETIREMENT SOLUTIONS | TECHNOLOGY | SEPTEMBER 26, 2017

On August 7, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a risk alert containing observations from its Cybersecurity 2 Exam Initiative. As a follow-up to the 2014 Cybersecurity 1 initiative, the Cybersecurity 2 Initiative examined the cybersecurity preparedness of 75 SEC-registered broker-dealers, investment advisers, and investment companies (funds) for the period of October 2014 through September 2015. In its report, OCIE identified issues of continuing concern, and articulated some best practices recommendations.

Overall, OCIE noted an observable increase in examined firms' cybersecurity preparedness in comparison to the prior examination. All broker-dealers, all funds, and nearly all investment advisers now maintain written cybersecurity policies and procedures. To varying degrees, a majority or many of the examined firms: conduct periodic risk assessments; conduct penetration tests and vulnerability scans (although they did not always remediate the weaknesses identified); have tools to prevent, detect, and monitor data loss; maintain processes to ensure regular system maintenance (although patches are not always installed immediately); maintain cybersecurity organizational charts; have obtained authorization from customers and/or shareholders to transfer funds to third-party accounts; and require vendor risk assessments or risk management and performance reports.

Despite that progress, OCIE highlighted three persistent issues. First, policies and procedures are often not reasonably tailored to the firm or risk, instead offering general or vague guidance and limited examples of appropriate safeguards. Next, firms maintain policies and procedures but neglect to meaningfully enforce compliance with them, or such policies and procedures fail to accurately reflect the firms' actual practices. For instance, annual reviews are not conducted annually, ongoing reviews of security protocols are conducted only annually, or firms fail to ensure that employees attend required cybersecurity trainings. Finally, firms failed to adequately maintain their systems as related to Regulation S-P, for example by neglecting to install software security patches, using outdated operating systems, or not conducting appropriate remediation efforts in response to risk assessments.

The risk alert concluded with OCIE's identification of so-called "robust" policies and procedures for firms to consider, including:

- maintaining a complete inventory of data, information, and vendors;
- maintaining detailed instructions regarding penetration tests, security monitoring, system auditing, rights of access to information, reporting, and other cybersecurity-related protections;
- maintaining strict processes regarding data integrity and vulnerability tests, including prescriptive testing schedules, beta-tests of security patches and other solutions, and prioritization of corrective actions for identified vulnerabilities;
- establishing data and system access controls and enforcing those controls;
- imposing mandatory employee training requirements and instituting procedures to ensure those training requirements are satisfied; and
- maintaining active engagement by senior management officials with all cybersecurity policies and procedures from formulation to enforcement.

While OCIE emphasized these policies as options to consider to improve cybersecurity preparedness, throughout the risk alert it noted that the examinations revealed that untailored policies or general guidance were causes for concern. Affected firms in the industry should not expect that blindly adopting the best practices identified by OCIE will constitute a safe harbor, nor necessarily constitute the most secure approach for every individual firm. Firms should conduct thorough reviews of their policies and procedures in light of their everyday practices, individual circumstances, and current and developing threats to assess their cybersecurity preparedness. Reliance on off-the-shelf and generic boilerplate language is insufficient. This recent initiative built on the Cybersecurity 1 Initiative and involved more validation and testing of procedures and controls.

Registered entities should prepare for additional validation and testing in any future SEC examination initiatives.