CLIENT ALERT

SEC Announces Guidance on Cybersecurity Exam Focus Areas

Sep.18.2015

On September 15, 2015, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert specifying cybersecurity examination focus areas for broker-dealers and investment advisers. Following up on the February 2015 OCIE Risk Alert that we described here, this Risk Alert cautions that examiners will evaluate how firms test and implement tailored cybersecurity policies and procedures.

The Risk Alert includes a sample list of information that OCIE may request in advance of an examination. Compliance professionals should familiarize themselves with this list to ensure the establishment and implementation of appropriate policies, procedures, and risk management infrastructure.

Key Takeaways

Firms should expect that examiners will review the following documentation:

- **Governance and Risk Assessment**: Records evidencing periodic evaluation of cybersecurity risks, tailored controls and risk assessment processes, and the active involvement of senior management and boards of directors.
- **Access Rights and Controls**: Records evidencing that firms control access to various systems and data via management of user credentials, authentication, and authorization methods. Records should demonstrate that firms have reviewed controls associated with remote access, customer logins, passwords, firm protocols to address customer login problems, network segmentation, and tiered access.
- **Data Loss Prevention**: Records evidencing monitoring for potentially unauthorized data transfers and proactive verification of the authenticity of a customer request to transfer funds. Firms should be able to monitor the volume of content transferred outside of the firm by its employees or through third parties, such as by email attachments or uploads.
- **Vendor Management**: Records relating to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight, and contract terms. Firms should evaluate vendor relationships as part of their ongoing risk assessment process and determine the appropriate level of due diligence to conduct on a vendor.
- **Training**: Records evidencing training tailored to specific job functions and encouragement of responsible employee and vendor behavior. Proper procedures for responding to cyber incidents under an incident response plan must be integrated into regular personnel and vendor training.
- **Incident Response**: Records detailing the establishment and testing of policies, response teams, assigned roles, assessed system vulnerabilities, and developed plans to address possible future events. To the extent an incident response team is called to action, records should detail what the team accomplished. Firm records also should demonstrate an understanding as to which firm data, assets, and services warrant the most protection to help prevent attacks from causing significant harm.

Conclusion

Cybersecurity has been a theme of increasing importance that Crowell & Moring follows closely. Broker-dealers and investment advisers should be on notice that regulators expect them to maintain up-to-date policies and tailored procedures to mitigate cybersecurity threats. Firms also should maintain documentary evidence of periodic testing of such policies and procedures. In their February 2015 cybersecurity guidance, OCIE, and FINRA regulators indicated that they did not expect that small and medium sized firms would have adequate in-house resources to fully address cybersecurity challenges. Given the lack of comprehensive and affordable third party vendor solutions, small and medium sized firms may be hard-pressed to meet regulatory expectations.

Additional information about Crowell & Moring's cybersecurity practice may be found here.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com