BACK PAGE FRONT BURNER

SEC is Serious About Cybersecurity Compliance

By Jeffrey Taft, Matthew Rossi and Amy Ward Pershkow

CYBER RISKS FACED BY THE U.S. financial markets have been front page news over the last few months. This September, the SEC announced that its online database for receiving, storing, and publishing corporate securities filings had been compromised in 2016 by hackers who may have traded on information they obtained. Two weeks earlier, Equifax announced that it was the victim of a cyber attack. Before that, businesses around the world were attacked by WannaCry ransomware.

In light of these and similar cyber events, all businesses should review their cybersecurity policies and procedures.

In August, the SEC's Office of Compliance Inspections and Examinations (OCIE) announced the results of its second cybersecurity examination initiative. For about a year beginning in September 2015 OCIE examined 75 regulated entities — broker-dealers, investment advisers, and investment companies — focusing on governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.

OCIE reported the results of its initiative in a "Risk Alert," which recommends best practices for regulated entities. Six elements that regulated entities should consider adopting as part of their compliance plan were identified:

- **Maintenance of an inventory of data, information and vendors:** A complete inventory and classification of the related risks and vulnerabilities.
- **Detailed policies and procedures for penetration testing, security monitoring, system auditing, access rights and data breach reporting:** Specific documentation addressing the scope, methodology, timing and responsible parties for cybersecurity activities.
- **Maintenance of schedules and processes for activities such as vulnerability scanning and patch management:** Defined schedules and prioritization for identifying system vulnerabilities.
- **Effective access controls and access monitoring:** Implementation of acceptable use and mobile device policies, review of third-party vendor logs and very prompt termination of former employee systems access.
- **Mandatory enterprise-wide information security training:** Periodic and onboarding training covering all employees.
- **Engagement of senior management in the review and approval of cyber-related policies and procedures.**

The OCIE has indicated that it will continue its initiative by examining cybersecurity compliance procedures and controls, and their implementation at regulated entities.

The SEC's focus on cybersecurity is not limited to regulated entities. It has also addressed cybersecurity for issuers of public securities. In 2011, the SEC's Division of Corporation Finance released guidance explaining that existing disclosure requirements may impose an obligation to disclose significant cybersecurity risks and incidents.

Companies should consider whether cyber risks or incidents should be disclosed in prospectuses, registration statements, and the "Description of Business" and MD&A sections of their periodic filings. Disclosures about cybersecurity matters are not required in such detail that they would compromise cybersecurity efforts.

In addition, the SEC has targeted cybersecurity violations in enforcement actions. In particular, the Division of Enforcement has focused on the "safeguards rule," adopted in 2000 as part of Regulation S-P under the Gramm-Leach-Bliley Act. Recent enforcement actions targeting violations of the safeguards rule show that the SEC is serious about cybersecurity compliance. ■