Securities Regulation Daily Wrap Up, TOP STORY—SEC chairman reveals cyberattack on EDGAR system, (Sept. 21, 2017)

Securities Regulation Daily Wrap Up

Click to open document in a browser

By Jacquelyn Lumb

SEC Chairman Jay Clayton released a statement last evening in which he revealed that a 2016 cyberattack on the SEC's EDGAR test filing system enabled a hacker to gain access to nonpublic information. The Commission patched the software vulnerability in August 2017 after learning that the attack may have provided an opportunity for illicit gains through trading. Clayton advised that the SEC does not believe the intrusion resulted in unauthorized access to personally identifiable information, or that it jeopardized operations or resulted in systemic risk. The investigation is ongoing and Clayton said the SEC is coordinating with the appropriate authorities.

Clayton reported that he has created a senior level cybersecurity working group to coordinate information sharing, risk monitoring, and incident response. He ordered an assessment of the SEC's approach to cybersecurity in May. In the statement he released last night, he described the SEC's approach to cybersecurity including how it manages risks and how it responds to cyber events related to its operations. The SEC plans to discuss internal cybersecurity matters in its annual agency financial reports going forward.

Data protection. The SEC receives, stores, and transmits data under three broad categories, Clayton explained. For example, it collects and makes publicly available information filed by issuers and other registrants through its EDGAR system. The second category includes nonpublic information related to its supervisory and enforcement functions, and the third category relates to internal operations such as personnel records. In the second category, Clayton noted that the consolidated audit trail, once launched, will contain significant, nonpublic, market sensitive data and personally identifiable information, so cybersecurity is a key element in its development.

Like many government agencies, financial market participants, and other private sector entities, Clayton said the SEC is subject to frequent attempts to disrupt its systems, access its data, or damage its technology infrastructure. He reported that the SEC has investigated and filed cases against individuals who allegedly submitted fake filings on EDGAR in an attempt to profit from the resulting market movements.

Internal threats. The SEC also faces risks of unauthorized actions or disclosures by its own personnel. Clayton reported that a 2014 internal review found that laptops which may have contained nonpublic information could not be located. Internal reviews have also uncovered instances where personnel transmitted nonpublic information through email accounts that were not secure.

New measures. The SEC has a detection, protection and prevention program, but Clayton noted that cybersecurity is an evolving landscape in which the SEC is constantly learning from its experience and that of others. Although there are limits on its hiring, he said the SEC expects to add expertise in this area. He also reported that the SEC is in the process of implementing the National Institute of Standards and Technology framework for improving critical infrastructure cybersecurity.

Going forward, Clayton said the SEC regularly reviews whether its data protection protocols are appropriate with respect to the sensitivity of the data it collects and the risks of unauthorized access. The SEC regularly evaluates whether there are alternatives that may reduce the sensitivity of the data it collects, such as collecting it on a delayed basis when appropriate.

Piwowar statement. Commissioner Michael Piwowar also released a statement last evening advising that he was recently informed for the first time about the 2016 EDGAR intrusion. He expressed support for the

investigation that is underway in order to fully understand the scope of the intrusion and ways to better manage cybersecurity risks to the SEC's operations.

MainStory: TopStory SECNewsSpeeches CyberPrivacyFeed RiskManagement