SEC Releases Results of Cybersecurity Exam Sweep

Digital Media and Data Privacy Law Blog

on 03.15.2015
Posted in Data Breach, Data Security

Ed. Note: This entry is cross posted from Cady Bar the Door, David Smyth's blog offering Insight & Commentary on SEC Enforcement Actions and White Collar Crime.

We're behind on this, but better (a little bit) late than never. Last month the SEC's Office of Compliance, Inspections and Examinations released the first results of its Cybersecurity Examination Initiative, announced in April 2014. As part of the initiative, OCIE staff examined 57 broker-dealers and 49 investment advisers to better understand how these entities "address the legal, regulatory, and compliance issues associated with cybersecurity."

What the Exams Looked For

In the exams, the staff collected and analyzed information from the selected firms relating to their practices for: identifying risks related to cybersecurity; establishing cybersecurity governance, including policies, procedures, and oversight processes; protecting firm networks and information; identifying and addressing risks associated with remote access to client information and fund transfer requests; identifying and addressing risks associated with vendors and other third parties; and detecting other unauthorized activity.

Importantly, the report is based on information as it existed in 2013 and through April 2014, so it's already somewhat out of date.

The Good News

The report includes some good news about how seriously the SEC's registered entities are taking cybersecurity.

· The vast majority of examined broker-dealers (93%) and investment advisers (83%) have adopted written information security policies.

· The vast majority of examined broker-dealers (93%) and investment advisers (79%) conduct periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences.

· The vast majority of examined firms report conducting firm-wide inventorying, cataloguing, or mapping of their technology resources. Smart.

· Many firms are utilizing external standards and other resources to model their information security architecture and processes. These include standards published by National Institute of Standards and Technology ("NIST"), the International Organization for Standardization ("ISO"), and the Federal Financial Institutions Examination Council ("FFIEC").

Encouraging! But the report didn't bring all good tidings.

The Bad News

Here are some of the less auspicious facts:

· 88% of the broker-dealers and 74% of the advisers reported being the subject of a cyber-related incident.

· Most of the broker-dealers (88%) require risk assessments of their vendors, but only 32% of the investment advisers do.

· Related to that, most of the broker-dealers incorporate requirements relating to cybersecurity risk into their contracts with vendors and business partners (72%), but only 24% of the advisers incorporate such requirements. Fewer of each maintain policies and procedures related to information security training for vendors and business partners authorized to access their networks.

· A slight majority of the broker-dealers maintain insurance for cybersecurity incidents, and only 21% of the investment advisers do.

The Rest

Almost two-thirds of the broker-dealers (65%) that received fraudulent emails seeking to transfer funds filed a Suspicious Activity Report with FinCEN, as they're likely required to do. The report then notes that only 7% of those firms reported the incidents to other regulators or law enforcement. It's curious to me why the SEC would expect other reports to happen. With the SAR obligations in place, those firms probably, and reasonably, think all the necessary reporting has been done after the SAR has been filed. Also, these firms' written policies and procedures generally don't address whether they are responsible for client losses associated with cyber incidents. Along these lines, it might be that requiring multi-factor authentication for clients and customers to

access accounts could go a long way toward pushing responsibility for those losses on the users.

But don't take my word for it. Read the report yourself, linked above and here.