The SEC's Investment Management Division Has

Digital Media and Data Privacy Law Blog

on 07.24.2015
Posted in Cyberattack, Data Breach

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.

Lots of agencies and organizations want to boss you around about cybersecurity. In April, the SEC and the Justice Department published more directions on the issue. We'll cover the very brief guidance issued by the SEC's Division of Investment Management first, and then turn to DOJ in a later post.

First, as with everyone else, the IM Division thinks cybersecurity is very, very important for investment companies and investment advisers.

Second, the staff recommended that advisers and funds consider a number of measures to strengthen cybersecurity:

· Conduct a periodic risk assessment.

· Create a strategy designed to prevent, detect and respond to cybersecurity threats. Specific pieces of the strategy could include: tiered access to sensitive information and network resources; data encryption; restricted use of removable storage media; and development of an incident response plan.

· Implement the strategy through written policies and procedures and training that provide guidance to officers and employees. Then monitor compliance.

· Assess whether protective cybersecurity measures are in place at relevant service providers.

This is a truncated list, and it isn't magical. The suggestions could apply to literally any business. You can read the full version here, but FINRA is way ahead of the Investment Management Division in providing usable guidance on how to bolster cybersecurity.

Third, and more interestingly, the guidance suggests that funds and advisers should take their compliance obligations under the federal securities laws into account in assessing their ability to prevent, detect and respond to cyber attacks. So, maintaining a compliance program that is reasonably designed to prevent violations of the securities laws could also mitigate exposure to

cyber threats, the guidance says. “For example, the compliance program of a fund or an adviser could address cybersecurity risk as it relates to identity theft and data protection, fraud, and business continuity, as well as other disruptions in service that could affect, for instance, a fund’s ability to process shareholder transactions.” In other words, if a cyber attack prevents you from, say, being able to process shareholder transactions, the staff is going to look back and see how well prepared you were before the assault. If you weren't prepared at all, the end result probably won't be pretty, for the shareholders or you.

The guidance recognizes that it’s impossible to anticipate and prevent every cyber attack. But it wants you to try. And appropriate planning could mitigate the impacts of those attacks, as well as help “compl[iance] with the federal securities laws.” Consider yourself warned.