Published on *The National Law Review* https://natlawreview.com

SEC's Most Recent Cybersecurity Move: What Registered Investment Advisors Need to Know

Article By:

Brian A. Bullard

Gregory M. Kratofil, Jr.

As public concern over data security grows in the wake of the Equifax data breach, the U.S. Securities and Exchange Commission (SEC) is increasing its scrutiny of registered investment advisors (RIAs). **In turn, RIAs should take additional steps to protect their businesses and clients.**

In a recent Risk Alert, the SEC stressed that its proposed measures were suggestions and not requirements at this point, although **RIAs should be proactive and prepare for the possibility that new regulations could be on the way.**

The Office of Compliance Inspections and Examinations (OCIE) of the SEC recently released a Risk Alert that detailed its examination of the cybersecurity preparedness of 75 broker-dealers, investment advisers and investment companies in the United States. In comparison to prior cybersecurity examinations, this exam involved more active testing and validation of the firms' procedures and controls related to cybersecurity.

Common Weaknesses

The SEC found two overarching themes. **First, it found that firms were better prepared during this examination than during the 2014 Cybersecurity Initiative exams. Second, the staff found that investment adviser firms tended to be less prepared than broker-dealers in some areas examined, such as penetration testing and data breach notification.**

The staff noted three main areas of weakness across firms:

> **Cybersecurity policies too general or vague to be useful to the firm's employees.** Investment adviser firms should develop procedures that give specific, not merely general, guidance. To maximize employee comprehension and adherence, an investment adviser firm's policies and procedures should include concrete examples and specific procedures tailored to the firm's practices.

Failure to enforce or to tailor cybersecurity policies to the firm's needs. This risk is not limited to an investment adviser firm's cybersecurity practices; a firm without cybersecurity policies and procedures adequately tailored to its needs may also have similar deficiencies throughout its compliance program.

Inadequate maintenance of information technology systems. Some examinees were found to be using outdated operating systems or other software that was no longer supported with security updates by the manufacturer. Running software without security updates leaves an investment adviser vulnerable to otherwise avoidable cybersecurity losses. Furthermore, the staff found situations in which some examinees had identified vulnerabilities during cybersecurity testing but failed to take action to remediate their findings.

SEC Guidance

The SEC staff highlighted three main actions that an RIA firm could take to help address information technology security issues:

- Conduct a periodic information technology security risk assessment.
- Create and test a strategy that is created to "prevent, detect and respond to cybersecurity threats."
- Implement the strategy by creating written policies and procedures and training internal staff and possibly clients.

The staff further suggested that assessing information technology security risks should be a critical part of a firm's annual compliance risk assessment. The logic of the argument is that **it's hard to successfully design a cybersecurity strategy without first taking a step back and identifying the key threats and vulnerabilities that are unique to a particular advisory firm.**

When crafting an information technology security strategy, the staff noted that some of the key focus areas of that strategy may include:

1. Access control to systems and sensitive data
2. Encryption
3. Restricting the use of removable storage media
4. Having the ability to monitor network activity for unauthorized intrusions
5. Data backup and retrieval
6. Creation of an incident response and business continuity plan

Going Forward

Even though the SEC has not issued any regulations, it is clear that cybersecurity will remain a priority. It should be for RIA firms, too. **The North American Securities Administrators Association is mulling a model cybersecurity rule for investment advisors and is currently developing cyber guidance and a "checklist" for small advisory firms to use to assess their cyber preparedness.**

Firms can also incorporate the elements present in the policies and procedures of firms the SEC determined had the most robust cybersecurity programs. These include:

- Keeping a detailed inventory of data, information and vendors
- Giving specific instructions in the policies and procedures, including examples where helpful
- Regularly testing technology systems and implementing cautious but timely security patch deployment to all machines
- Establishing and enforcing controls for access to firm data or systems, such as acceptable use policies, mobile device management, vendor activity logs detailing use of the firm's system and immediate elimination of system access for terminated employees
- Mandatory employee training, both upon hire and periodically throughout the year
- Active engagement by senior management

National Law Review, Volume VII, Number 300