2021 SEC Exam Priorities: Cybersecurity, Access Management & Remote Workforce

June 21, 2021

By Wes Stillman

EXAMS, or what’s now known as the at the Securities and Exchange Commission (SEC), recently issued this year’s priorities for advisor examinations. Advisors who want a better understanding of how the SEC’s Division of Examinations (EXAMS) is shifting its focus would do well to read the full report themselves, as there’s a lot of good information packed into those 42 pages. But for those who are pressed for time, I thought I’d recap my takeaways on RIA cybersecurity here.

After spending more than a year working remotely in some way, its no surprise that this year’s exam places greater scrutiny on remote work and related technologies. EXAMS wants to see whether RIAs have updated policies and procedures that are reasonably designed, implemented and enforceable for today’s world.

This includes a look at whether an RIA’s cybersecurity protocols reflect the way the firm works now, versus when the protocols were first developed. Examiners want to see whether RIAs have adequate cybersecurity protocols in place and actively enforced, so that access from anywhere and from any device remains secure, keeping firm and client data protected.

A Closer Look at Access Management

Secure access management – that is, how firms control access to all key systems, devices and data – has been a periennial concern of the SEC. But as all of us have collectively shifted to an increasingly remote workforce , EXAMS is now shining an even brighter light on access management.

This means it is critical for advisors to close lingering gaps between remote work, end device management and home networks with their existing cybersecurity policies.

That said, it’s difficult to buy company devices for all employees and it’s even harder to mandate control over personal devices. Cloud-based IT management and virtual desktops can help facilitate file sharing and face-to-face (if not in person) meetings using Microsoft Teams, Zoom and similar applications, but access to all of these tools must be secured.

Digging Into Access Management

In the year ahead, RIAs, should periodically review their cybersecurity policies and programs, paying special attention to updating password policies so they are consistent with industry standards. Reviews should be conducted annually, at a minimum –ideally they would be done more than once a year.

For example, it is no longer simply enough to use Multi-Factor Authentication (MFA) to validate an individual who is seeking to log into an account. In a remote work environment, MFA should be used in combination with conditional factors and defenses, such as a Remote Desktop Protocol (RDP) that is supported through an encrypted known connection,. Additionally, the use of technologies to control and monitor access to the Internet can address potential security vulnerabilities of Internet connections.

Since cybersecurity attacks and data breach attempts are increasing in frequency and sophistication, EXAMS also wants to understand how RIAs and their third party service providers plan to respond when

(not if) these events happen. Examiners are looking for the gold standard in cybersecurity incidence response: the 1-10-60 protocol. That's one minute or less to detect, 10 minutes to investigate, and 60 minutes to remediate. Any protocol that is less rigorous is considered sub-par and falls outside of SEC guidance.

Governance, risk and compliance (GRC) tools can help firms manage these rIsks; in fact, RightSize is currently piloting a GRC solution for RIAs that will be available later this year.

The new EXAMS priorities report makes clear that in 2021, examinations will focus on how firms are controlling access in a remote environment, and whether their day-to-day operations are consistent with their representations. In short, does your firm's cybersecurity walk match up with your cybersecurity talk? The time to figure this out it now.