RICHEY MAY | Alternative Investments

Are You SEC Cybersecurity Ready?

A Guide for Fund Managers

In late 2024, the SEC Division of Examinations announced its 2025 Priorities. With this, the SEC has introduced new cybersecurity rules for Registered Investment Advisers (RIAs) that significantly enhance their cybersecurity obligations. These regulations may signal new cybersecurity standards for the financial industry as a whole in the future, both from the SEC and at the state level. **These trends result in one question for RIAs and non-RIAs alike: are you SEC cybersecurity ready?**

The SEC's focus on cybersecurity highlights the best practices that can protect your fund and investor data, including:

Risk Management Policies

Even unregistered advisers are encouraged to implement cybersecurity policies to manage risks effectively.

Incident Response Plans

Developing and testing incident response plans can reduce the impact of a cybersecurity related incident or breach, such as ransomware.

Third Party Risk Management

While you may exclusively utilize Cloud and SaaS platforms for your technology, this doesn't mean you've outsourced your risk. The SEC is placing an emphasis on ensuring you practice your own due diligence when engaging with third parties.

While the SEC will be the main governing body for these requirements, investors increasingly expect robust cybersecurity measures as well, to ensure their personal data, interests, and funds are protected, regardless of registration status.

Risk Assessments

One of the fundamental requirements for SEC RIAs is to conduct regular risk assessments that align with a cybersecurity risk management framework (CRMF). **Regardless if you are a SEC RIA or not, a CRMF is a playbook you can use to identify, assess, and mitigate your cybersecurity risk. It is not about just reacting to threats as they arise; a CRMF helps you plan for future requirements.**

Written Policies and Procedures

SEC RIAs are required to establish and maintain written cybersecurity policies and procedures. This is a best practice for all fund managers, regardless of the size or type of fund. These documents should outline the fund's approach to managing cyber risks, including the measures in place to protect client and investor information and reduce the potential liability of an incident. Policies should cover areas such as data encryption, access controls, network security, and incident response.

Employee Training and Awareness

Employees need to understand the threats that they are facing in the workplace. Consistent and measurable training is important for fund managers to have in place. The ways in which threat actors are attempting to gain information from organizations continue to evolve, so it is imperative that the training and awareness programs help give employees tools to recognize and report attempted attacks.

Access Controls

SEC RIAs must implement robust access control measures, such as multi-factor authentication (MFA), role-based access controls (RBAC), and regular reviews of user access privileges. Limiting access to only those employees who need it to perform their duties reduces the risk of data breaches and unauthorized data manipulation – this is a best practice for any size fund. Employees should only ever be given the minimum amount of access to do their assigned job functions.

Data Encryption

Data encryption is a best practice vital component of any cybersecurity strategy. SEC RIAs must ensure that sensitive information is encrypted. This means that data should be protected when it is being transmitted over networks and when it is stored on servers or devices. Encryption makes it significantly more difficult for cybercriminals to access and exploit sensitive information.

Incident Response Planning

Despite best efforts, cyber incidents can still occur. **SEC RIAs must have a detailed incident response plan in place, especially for Ransomware**. This plan should outline the steps to be taken in the event of a cyberattack, including how to contain the breach, assess the damage, and communicate with affected parties. An effective incident response plan helps any size or type of fund minimize a breach's impact and ensures a swift recovery. These plans should be tested and refined annually.

Be SEC Ready with a Modern Compliance Management Platform

Effective compliance management is a critical component of any fund's operations, particularly when it comes to meeting SEC RIA cybersecurity requirements. Managing these new requirements via a manual spreadsheet, especially as these requirements grow in complexity, is challenging and will only get more difficult in the future. In the event of an SEC audit, fund managers who use manual methods may struggle. Being SEC cybersecurity ready means fund managers should be able to confidently provide auditors with access to a dedicated portal, streamlining the process of demonstrating compliance adherence.

To answer this need, Richey May has developed a unique and innovative SEC RIA Cybersecurity Compliance Automation Framework using Drata, a leading industry platform. This

Additionally, the platform includes a digital Trust Center, serving as a consolidated resource for interested parties such as cybersecurity insurance providers and potential investors seeking information about the fund's security measures.

comprehensive solution offers centralized management and updates for policies and procedures, while also facilitating third-party vendor management. The framework provides a valuable comparison against SEC RIA Compliance requirements, ensuring that firms stay up to date with regulatory standards.

Complexity in cybersecurity regulations will continue to grow. Be SEC cybersecurity ready by following these best practices and get expert guidance. Richey May's full technology and cybersecurity support services enable fund managers to focus on their core operations and funding activities, rather than getting bogged down in compliance details.

Talk to us. Richey May specializes in audit, tax, cybersecurity, and accounting services for the alternative investments industry. If you need further guidance, reach out to **Steve Vlasak**, Business Development Partner, Alternative Investments Practice.