The SEC's Cybersecurity Risk Management Rule: Your Cheat Sheet for Preparedness

Overview of The Cyber Rule's Top Four Requirements

The SEC's proposed Cybersecurity Risk Management Rule is set to be approved this year by the Commission and creates an entirely new cybersecurity compliance regime for asset managers and the wider alternative investment management sector.

Together, trusted global managed service provider (MSP) to over 1,000 alternative investment firms, ECI, and esteemed investment management law firm, Cole-Frieman & Mallon LLP, have created this quick and comprehensive guide to empower asset managers with the requisite legal and IT considerations to build, monitor and continuously adapt their cybersecurity defenses to comply with the rule. Cybersecurity is truly a multi-factorial challenge that requires a multi-disciplinary approach. Cybersecurity compliance is not a project but rather a continuous process that contemplates methodical and reasonable steps that mature your cybersecurity posture over time.

1. Design and Implement Cybersecurity Policies and Procedures

This is by far the most comprehensive of the four requirements, creating the heaviest lift for asset managers. Salient points are:

A. This goes beyond the typical requirement of a passive "written policy" document and calls for:

- Creating Policies and Procedures, tailored and appropriately scaled;
- Conducting Cybersecurity Assessments, conducted at least annually; and
- Preparing an Annual Written Report.

B. Taken together, the "policies and procedures" requirement of the Cyber Rule sets out the framework of what the SEC considers to be a Model Cybersecurity Program, which is essentially a dynamic combination of: well-tailored and fluid written policies; a specifically configured IT infrastructure; distinct, finely tuned technological controls; and appropriate and periodic operational procedures (such as Cybersecurity Assessments and the Annual Written Reports), that all focus on security.

Legal tip:
A model cybersecurity program is expected to be appropriately scaled and commensurate with each asset manager's particular resources and unique capabilities. Boilerplate, template and non-customized policies should be avoided and have been the cause of regulatory fines and penalties in each and every SEC cybersecurity enforcement action.

IT tip:
An industry-specific and experienced MSP can support asset managers by taking on the responsibility of configuring and fine tuning its IT infrastructure and in regularly conducting the required cybersecurity control tests and providing the corresponding ongoing reporting.

2. Reporting Cybersecurity Incidents to the Commission

This is an entirely new regulatory reporting obligation. Salient points are:

- Managers will be required to report certain cybersecurity incidents to the SEC on newly created schedule Form ADV-C within 48 hours from having a reasonable basis to conclude such an incident; and
- This new reporting requirement is triggered only with cybersecurity incidents that either: (i) impair the firm's critical operations; or (ii) lead to access of information that substantially harms the firm or any investors.

Legal tip:
A cyber reg-reporting requirement is unprecedented and a feature of the SEC's new and aggressive cyber compliance regime. Form ADV-C completion will require thoughtful attention and reliance on both the IT and legal functions. The 48-hour reporting window has received significant industry pushback.

IT tip:
Understanding cyber incidents with a Managed XDR (Extended Detection and Response) program is now the expected standard from both the SEC and ODD firms alike. To report on cyber incidents, you will need a firm understanding of your environment as well as the threat landscape. Having a robust Managed XDR program in place is the key to understanding how, when and why threats occur, thus enabling firms to provide a comprehensive report on incidents. Not having a well thought out program can increase your chances of facing a fine.

3. Disclosure of Cybersecurity Risks and Incidents to Investors

This is also an entirely new disclosure obligation that requires managers to:

- Disclose cybersecurity risks on Form ADV Part 2A Brochure, including general cyber risks that are material and cyber incidents over the past two fiscal years; and
- Prepare interim amendments to the brochure, in certain cases.

Legal tip:
This new disclosure obligation will require managers to be more aware of, and engaged with, their cybersecurity risk posture in order to determine when such disclosures are necessary.

IT tip:
Like the first requirement, firms are encouraged to build strong cyber defense policies, detection capabilities and related procedures and be prepared to continuously adapt them to the landscape and its unique day-to-day operations. Even the most proactive firms deal with attacks. Therefore, it is important to be able to identify gaps, build effective remediation plans, and be able to report on them.

4. Recordkeeping

This is also an entirely new requirement but the most linear of all requirements.

- The retention period is five (5) years and relates to documents regarding cybersecurity risk management practices, cybersecurity incidents and incident response; and
- This new recordkeeping requirement contemplates a broad scope of what documents need to be retained and includes all cybersecurity policies, assessments and annual written reports, as well as documents regarding each cybersecurity incident.

Legal tip:
This new recordkeeping obligation essentially expands the current books and records rule to include all the documents expressly required by the rule, as well as documentation regarding incidents. This requirement is yet another clear example of how the new Cyber Rule is creating a more formal and intensive cybersecurity compliance regime.

IT tip:
As a best practice, MSPs recommend having a platform that stores all data and tracks changes to comments and historical logs. This could become an audit point further down the line but is also a prudent practice to help you track the evolution of your cyber risk profile.

For more information on preparing for the SEC's Cyber Risk Management Rule, please reach out to us.

ECI - www.eci.com | +1 800 752 1382

Cole-Frieman & Mallon LLP
John T. Araneo, Partner
jaraneo@colefrieman.com
(415) 762-8702