Salus GRC

September 2023

Contact: Jacob Cane jcane@salusgrc.com

SEC's Proposed Cybersecurity Risk Management Rules: Implications for Private Funds and Investment Advisers

In recognition of the escalating cybersecurity threats faced by financial entities and the potential risks posed to investors and financial markets, the U.S. Securities and Exchange Commission (SEC) has proposed new cybersecurity risk management rules. The proposal includes new rule 206(4)-9 under the Advisers Act, new rule 38a-2 under the Investment Company Act and amendments to Rule 204-2 of the Advisers Act. Expected to be finalized in October 2023, these regulations will mandate that investment firms demonstrate compliance through comprehensive information security controls, policies, and oversight.

Why It *Really Is* Different This Time

These regulations represent a major shift in the cybersecurity landscape for SEC registered firms. While the SEC brought cybersecurity to the forefront with the April 15, 2014 OCIE Risk Alert and in subsequent communications, up until now much of the SEC's guidance on cybersecurity has been just that, guidance. Where rules do exist, cybersecurity is addressed in broad terms under other domains such as fraud prevention or fiduciary duty.

The proposed cybersecurity rules will have the full weight of SEC regulation and will be much more specific in their requirements. While the SEC wants to give firms some flexibility to tailor their cybersecurity programs to their business size and scope, for many program elements the SEC's language has shifted from "could" and "should" to "must" and "required".

Key Components of the Proposed Rules

The SEC's proposed cybersecurity risk management rules are designed to enhance the overall security posture of investment firms. These rules will require companies to adopt a comprehensive set of information security controls, policies, and oversight practices. Key components of the proposed rules include:

Risk Assessments:
Investment firms will be required to conduct regular risk assessments to assess, prioritize, categorize, and document cybersecurity risks. Risk assessments are foundational to an effective cybersecurity program and provide organizations with a baseline of their current cybersecurity posture and identify areas for prioritization. Risk assessments include these actions:

- **Assess Threats and Vulnerabilities:** Conduct a comprehensive risk assessment to identify potential threats and vulnerabilities that could compromise the security of your critical assets. Consider external threats like cybercriminals and nation-state actors, as well as internal threats like employee negligence.
- **Define Risk Tolerance:** Establish risk tolerance levels for different types of risks. This definition will help prioritize mitigation efforts and allocate resources effectively.
- **Document Formally:** Risk assessments must follow a formal process and be formally documented.
- **Provide Management Oversight:** Inform senior management of risk assessment findings regarding cybersecurity risks and action plans for remediation.

Information Security Policies:
Firms must develop and implement robust information security policies tailored to their specific risk profiles. These policies must be reviewed and updated annually. A robust policy program includes the following actions:

- **Develop a Policy Set:** Create a set of information security policies that cover all relevant areas. While an Incident Response Plan is the only policy specifically mandated by the SEC, generally accepted industry standards for a comprehensive cybersecurity policy set also include a Written Information Security Policy, Business Continuity Plan and Disaster Recovery Plan, and the proposed rules require information typically addressed in these policies.
- **Create Comprehensive Policies:** Information policies should include a wide range of best practice items including data protection, access controls, personal device policy, password management, incident response, vendor management, and employee training.
- **Address SEC Required Topics:** Information policies must also address areas specifically mentioned by the SEC including acceptable use, authentication management procedures (including multifactor authentication), timely distribution, replacement and revocation of passwords or methods of authentication, principle of least privilege and secure remote access.

- **Tailor Policies to Your Firm:** Customize the policies to align with your firm's specific risk profile, business processes, and IT infrastructure. One size does not fit all, and policies must be relevant and practical for your organization.
- **Implement a Review Process:** Establish a regular review process to ensure that your information security policies remain up-to-date and relevant to evolving cyber threats. The draft rules explicitly require that firms perform reviews at least annually.
- **Communicate Policies:** Educate all employees about the newly developed policies and their importance. Encourage a culture of security awareness and responsibility throughout the organization.

Service Provider Management and Assessment:
As many cyber incidents stem from vulnerabilities in third-party vendors, the proposed rules mandate investment firms maintain a strong service provider management program. This requirement includes conducting due diligence on vendors' cybersecurity practices and ensuring contractual obligations related to security are met through the following actions:

- **Inventory Service Providers:** Identify service providers that receive, maintain or process adviser or fund information, or that are permitted to access their information systems, including the information residing therein, and identify the cybersecurity risks associated with the use of these service providers.
- **Conduct Due Diligence:** Thoroughly assess the cybersecurity practices of all third-party vendors before engaging in business with them, including their data handling practices, information security policies, business continuity, and disaster recovery protocols, and risk management capabilities.
- **Include Security Clauses in Contracts:** Ensure that all contracts with vendors contain specific security clauses that outline their responsibilities and requirements concerning data protection and cybersecurity.
- **Monitor Vendor Performance:** Continuously monitor the security performance of your vendors throughout the engagement period. If any vendor's security practices fall short of expectations, take appropriate actions to mitigate risks.
- **Perform Regular Audits:** Conduct periodic audits of your vendors' cybersecurity measures to ensure ongoing compliance with your firm's security standards.

Threat and Vulnerability Management:

Advisers and funds are required to detect, mitigate, and remediate cybersecurity threats and vulnerabilities. While the SEC does not mandate the specific measures to use, recommendations in the rules include:

- **Establish Continuous Monitoring:** Threat and vulnerability monitoring systems should be configured to provide ongoing continuous monitoring wherever practical. Automated tools like intrusion detection systems, endpoint detection and security information and event management (SIEM) solutions can help with this task.
- **Conduct Vulnerability Assessments:** Systems and procedures should be implemented for monitoring, scanning, patching, and tracking of vulnerabilities.
- **Implement Threat Detection:** Advisers and funds generally should implement detection security capabilities that can identify threats on a network's endpoints.
- **Monitor Threat and Vulnerability Intelligence:** Advisers and funds generally should also monitor industry and government sources for new threat and vulnerability information that may assist them in detecting cybersecurity threats and vulnerabilities. Most threat and vulnerability management systems regularly receive intelligence updates from such sources.

Incident Response and Recovery:

The proposed rules emphasize the importance of a well-defined incident response and recovery strategy, including:

- **Create an Incident Response Plan:** Develop a comprehensive incident response plan that outlines the steps to be taken in case of a cybersecurity breach. This plan must address the continued operations of the fund or adviser, the protection of adviser information systems and the fund or adviser information residing therein, external and internal cybersecurity incident information sharing and communications and reporting of significant cybersecurity incidents to the Commission.
- **Regularly Test Procedures:** Advisers and funds should consider testing incident response procedures at least annually. Incident response testing is most commonly done by conducting tabletop exercises to simulate cyber incidents and test the effectiveness of your incident response plan. While testing itself is not mandated by the rules, advisers and funds are required to review and assess the design and effectiveness of the policies annually and testing is the most effective way to assess.

- **Form a Cybersecurity Incident Response Team:** Assemble a team to handle cybersecurity incidents promptly and effectively. Clearly define each team member's roles and responsibilities.
- **Establish Information Sharing Procedures:** Develop external and internal cybersecurity incident information sharing and communications plans and procedures.
- **Establish Reporting Procedures**: Set up clear reporting procedures to ensure that incidents are escalated to the appropriate management level and the SEC, if required, in a timely manner.

Employee Training and Awareness:

The human element remains a significant vulnerability in cybersecurity. While the proposed SEC rules do not contain clear mandated requirements on training, the rules make recommendations regarding training. Between their existing widespread adoption, past SEC recommendations and encouragement in the SEC rule, these items are typically viewed as de facto requirements in a cybersecurity program for SEC registered firms.

- **Develop Comprehensive Training Programs:** Create training programs that cover various cybersecurity topics, including phishing awareness, secure password practices, data handling, and incident reporting.
- **Conduct Regular Training Sessions:** Schedule periodic training sessions for all employees to reinforce the importance of cybersecurity and keep them informed about the latest threats and best practices. Annual training is an appropriate cadence for most firms.
- **Conduct Simulated Phishing Testing:** Regularly perform simulated phishing tests to gauge the effectiveness of cybersecurity training and increase cybersecurity awareness.
- **Promote a Culture of Security:** Encourage employees to take ownership of cybersecurity by fostering a culture where security is a shared responsibility. Offer incentives for reporting security incidents and following security protocols.

Reporting and Recordkeeping:

The proposed rules include multiple requirements for reporting and recordkeeping. For firms that already have robust cybersecurity programs in place, these requirements will require the most significant updates to their programs. While most of the requirements above are predominantly best practices already followed by many best in class advisers and funds, compliance with the reporting and recordkeeping requirements will require

substantial changes for nearly all firms. These requirements do not always follow well-established practices and several will demand new, as yet to be defined, forms or form amendments. Details in this domain are likely to be modified and better defined in the final rules and in additional guidance following the ratification of the rules.

The reporting and recordkeeping requirements will also encourage many firms to coordinate more closely between their cybersecurity programs and broader regulatory compliance programs, as information gathered through cybersecurity programs must often be reported through regulatory compliance channels.

- **Perform an Annual Review Report:** Review cyber policies and procedures at least annually in order to assess their effectiveness and design and determine whether they reflect changes in cybersecurity risk since the prior review. Write a formal report to describe the annual review, assessment, control tests performed and accompanying results, cybersecurity incidents, and policy changes since the last report.
- **Establish Incident Reporting Procedures:** The draft rules require firms to report significant cybersecurity incidents to the SEC within 48 hours of determining that a significant cybersecurity event has happened or is currently happening, or when new information is available.This reporting will be done via a newly created form, the ADV-C.
- **Establish Disclosure Procedures:** Advisers and funds will be required to disclose cybersecurity risks and incidents in plain English to investors, prospective investors and other market participants. Fund disclosure information must be provided in a structured data language (Inline eXtensible Business Reporting Language or “Inline XBRL”).Cybersecurity amendments are expected to be made to Form ADV Part 2A, Form N-1A, Form N-2, Form N-3, Form N-4, Form N-6, Form N-8B-2, and Form S-6.
- **Maintain Records:** Most firms must maintain and preserve books and records for a minimum of five years. Firms generally should maintain a copy of cybersecurity policies, assessments, and annual policy reviews, as well as the policies and procedures, from the last five years, a copy of any Form ADV-C or other incident report filed to the SEC in the last five years and records of any cybersecurity, including related response and recovery activities, from the last five years.

Board Oversight:
The rules explicitly require oversight of the cybersecurity program at a board level and specify that fund board oversight should not be a passive activity. Specifically, the fund board must:

- Approve and review the fund's cybersecurity policies and procedures.
- Review written reports to understand the fund's cybersecurity risk, incidents, and material changes to the fund's policies and procedures.
- Ask questions and seek clarification regarding program effectiveness, available resources, and cybersecurity expertise.
- Determine the level of oversight of service providers based on business operations.

Ongoing Programs:
The rules repeatedly emphasize that the SEC views cybersecurity program activities as part of an ongoing program with a regular cadence. Historically many managers address tasks such as risk assessments and policies as one-off projects or perform them on an ad-hoc schedule. Going forward, the SEC requires that these are performed on an ongoing basis.The frequency for most major items will be annual, whether that is explicit in the rule (policies) or implicit (risk assessments). In many cases where the frequency is not directly addressed in the rules, interdependencies with other tasks such as the annual report will provide a de facto frequency requirement.

Implications for Investment Firms
The SEC's proposed cybersecurity risk management rules will have several profound implications for investment companies and RIAs. While the intended purpose of these regulations is to enhance security and safeguard investor interests, firms will need to make substantial adjustments to their operations and infrastructure to achieve compliance. Here are some of the key implications for investment firms:

- **Increased Compliance Costs:** The implementation of robust cybersecurity measures will undoubtedly lead to increased compliance costs for investment firms. Firms will need to allocate resources for risk assessments, security infrastructure upgrades, policy development, employee training, and monitoring tools.
- **Heightened Focus on Cybersecurity:** The proposed rules will necessitate a greater focus on cybersecurity across all levels of the organization. Firms will need to establish dedicated cybersecurity teams, hire cybersecurity experts, and prioritize security-related initiatives

- **Competitive Advantage for Compliant Firms:** Firms that can swiftly adapt to the new regulations and demonstrate effective cybersecurity measures will likely gain a competitive advantage. Investors are increasingly prioritizing security and will be more inclined to invest with firms that can showcase strong cybersecurity practices.
- **Legal and Reputational Risks:** Failure to comply with the SEC's proposed rules could expose investment firms to legal repercussions and reputational damage. In the event of a cybersecurity breach, non-compliant firms may face penalties, litigation, and erosion of investor trust.
- **Collaboration with Third-Party Vendors:** Investment firms often rely on various third-party vendors for services. The proposed rules will require firms to closely collaborate with these vendors to ensure their cybersecurity practices align with the firm's security standards.
- **Increased Alignment between Cybersecurity and Regulatory Compliance:** The proposed rules situate cybersecurity requirements within the broader realm of regulatory compliance. This change will be most acutely felt in managing the regulatory/cybersecurity calendar and in regulatory filings but has further impact in other areas such as training and service provider management.
- **Continuous Compliance Efforts:** Cybersecurity is an ever-evolving field, and investment firms will need to continuously adapt their security measures to keep up with emerging threats and regulatory changes. Ongoing monitoring, risk assessments, and updates to policies will be necessary to maintain compliance.

What You Can Do to Prepare

Between the breadth of the proposed rules and the uncertainty of what may change in the finalized rules, it can be difficult to know where to start. Although many of the requirements are new or not fully defined, many others are best practices already recognized as effective by investors and regulators and practiced by many leading advisers and funds. These elements which form the core of robust cybersecurity program and are prominent elements of the SEC draft rules unlikely to change in the finalized version include:

- Risk assessments
- Policy development and review
- Service provider management and assessment
- Threat and vulnerability management
- Incident response planning and tabletop exercise testing

- User awareness and training
- Critical technical controls such as multifactor authentication and secure remote access

Action on these items will address the bulk of your preparation with minimal risk of duplicated or wasted effort when the rules are finalized. The risk assessment is the first task performed for most firms as it provides a baseline on cybersecurity readiness (including which other plan elements are already in place) and forms the basis of a prioritized plan of action for other efforts.

The next foundational step is to identify your team. Achieving compliance with the new regulations will require participation from a team of experts, including outside vendors, cybersecurity and compliance professionals, and internal stakeholders with a deep knowledge of your business and decision-making capability. Determining your internal champions and surrounding them with the support they need to succeed is the first step in this process

Contact:
Jacob Cane
Managing Director and
Head of Cybersecurity Risk Services
JCane@salusgrc.com