Salus GRC

September 2023

Contact: Jacob Cane jcane@salusgrc.com

The 3 Minute Guide to Preparing for the SEC Cybersecurity Rules

In October 2023 the SEC is expected to finalize new cybersecurity risk management rules: 206(4)-9 under the Advisers Act, 38a-2 under the Investment Company Act, and amendments to Rule 204-2 of the Advisers Act. The proposed rules were first introduced on February 9, 2022. Although the release has been delayed before, the SEC recently adopted a final cybersecurity rule for public companies and there is widespread consensus among industry experts that the private fund rules are likely to be finalized this October.

Balancing the need to prepare with the uncertainty of potential changes can be challenging. For those who wish to get ahead on preparation with minimal risk of unnecessary or duplicative effort, here are some steps you can safely take now:

1. Perform a Cyber Risk Assessment and Prioritize Risks. As the draft rules state, "[T]he first step in designing effective cybersecurity policies and procedures is assessing and understanding the cybersecurity risks facing an adviser or a fund." This exercise is fundamental to identifying and prioritizing risks. While the required frequency of risk assessments is still uncertain, the proposed rules make it clear that periodic assessments will be required.

2. Develop and Update Information Security Policies. Policies are another foundational element of any cyber security program. Annual updates to cyber security policies are one of the central tenets of the proposed rules and this requirement will almost certainly be unchanged in the final version. The proposed rules are explicit about multiple topics to address in the policies. While there is risk that the list of required topics may change in the finalized rules, all the topics mandated in the draft rules are best practices that are already adopted by some firms and should be adopted by all.

3. Ramp Up Service Provider Management. The proposed rules require firms to: inventory service providers with access to sensitive data or systems, assess the cybersecurity and resilience practices of these vendors, and include security clauses in contracts. As with cybersecurity risk assessments of advisers and funds, while the required frequency of service provider assessments is still uncertain, periodic assessments will be a requirement. Given the repeated emphasis in the draft rules and a separate SEC proposal for broader service provider oversight rules, there is little doubt that stronger service provider management practices will be required.

4. Evaluate Threat and Vulnerability Management. The requirement to "detect, mitigate, and remediate cybersecurity threats and vulnerabilities" is unlikely to be dropped from the final rules. For most firms, the best practice is to address threat management with their IT team or IT managed services provider and to implement vulnerability management through an independent third party such as a cybersecurity consultant.

5. Strengthen User Cybersecurity and Access Controls. Strong user access controls are not only a key component of the SEC rules likely to remain in the final version, but the most important measure in minimizing the likelihood of a breach. A cyber risk assessment will identify and prioritize improvements to your controls. The sooner your IT team is armed with this information the better, as adoption of improved controls can often be a long process.

6. Prepare an Incident Response Plan with Internal Reporting Procedures. The importance of incident response and the explicit requirement for incident response procedures are major themes in the proposed rules. Incident reporting and cybersecurity disclosure will be central requirements of the finalized rules, likely with significant penalties for non-compliance. Firms without a strong internal reporting capability will be unable to comply with external reporting and disclosure requirements. Some of the specifics on reporting procedures may be modified in the finalized rules, but it is safe to assume that there will be reporting requirements and that the first (and in most cases the most difficult) step in complying with them will be implementing strong practices for internal reporting of cybersecurity incidents to the CCO.

Where to Wait and See

The draft cybersecurity rules also strongly emphasize requirements around cybersecurity disclosures, recordkeeping, annual reporting, and board oversight. These will almost certainly be major components of the finalized rules and firms will need to adopt strong policies and procedures. These are also areas where specific requirements are relatively likely to change, implementation lead times are comparatively short, dependencies are favorable for later implementation and few firms already have mature programs. In other words, these areas both have more uncertainty and will be faster for firms with immature cybersecurity programs to "catch up" with their peers.

The proposed rules also contain many "could" and "should" recommendations. Some of these will likely become explicit requirements in the final rules, while many more are or will become de facto industry requirements (such as user awareness training). Best in class firms have already adopted many of these measures, but those who wish to limit their investment to requirements at this time may re-evaluate following the finalization of the rules.

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