# How Fund Industry Can Prepare For SEC's Cyber Proposal

By **Paul Ferrillo, Tracee Davis and Daphne Morduchowitz** (March 4, 2022)

Paul Ferrillo

Tracee Davis

Daphne Morduchowitz

On Feb. 9, the U.S. Securities and Exchange Commission issued new proposed rules related to understanding and mitigating cybersecurity risk for registered investment advisers, registered investment companies and business development companies.

SEC Chair Gary Gensler commented in a statement:

> Cyber incidents, unfortunately, happen a lot. Given this, and the evolving cybersecurity risk landscape, we at the SEC are working to improve the overall cybersecurity posture and resiliency of our registrants. ... Cybersecurity incidents can lead to significant financial, operational, legal, and reputational harm for advisers and funds. More importantly, they can lead to investor harm. The proposed rules and amendments are designed to enhance cybersecurity preparedness and could improve investor confidence in the resiliency of advisers and funds against cybersecurity threats and attacks.[1]

For many registered investment advisers and funds, a number of the rules are not surprising given yearly bulletins issued by the SEC's Division of Examinations that provide guidance to registered investment advisers and funds on what the SEC considers to be important issues.

But for many of these entities, some of the proposed rules might indeed be new, especially when it comes to mandatory incident reporting to the SEC.

Compliance with these and other rules will require a reevaluation of registrants' cybersecurity practices and policies.

This article provides an overview of the proposed rules and the key factors for considerations in their implementation.

We further note that given Gensler's desire to protect individual investors and improve their confidence in the marketplace, we would not be surprised if in the near future the SEC's proposed rules, as reviewed herein, were extended to also cover the public company sector.

This article aims to provide key insights for board directors, the C-suite and IT executives of registered investment advisers and funds, as well as for directors and officers of public companies.

### SEC Proposed Rule 206 (4)-9

To address the potential concerns that the easy way out has been taken by registered investment advisers and funds when it comes to cybersecurity, proposed Rule 206 would require advisers and funds that are registered or should be registered with the SEC to implement cybersecurity policies and procedures addressing a number of critical elements.

Further, the proposed rules would require registered investment advisers and funds to review and evaluate the design and effectiveness of their cybersecurity policies and procedures at least once a year, which would allow them to update those policies and procedures in the face of ever-changing cyber threats and technologies.[2]

The proposed rules are not, however, entirely clear as to what exact policies and procedures are required. But they are clear that registered investment advisers and funds must be attentive to cyber risks and implement policies to address them.

Rather than mandate specifics, the proposed rules are designed to give advisers and funds the flexibility to "address the general elements based on the particular cybersecurity risks posed by each adviser's or fund's operations and business practices," and to reassess cybersecurity risks and adjust cybersecurity policies and procedures accordingly to respond to ever-evolving cybersecurity risks and threats.[3]

The proposed rule further notes:

> Reasonably designed cybersecurity policies and procedures generally should specify which groups, positions, or individuals, whether in-house or third-party, are responsible for implementing and administering the policies and procedures, including specifying those responsible for communicating incidents internally and making decisions with respect to reporting to the SEC and disclosing to clients and investors certain incidents.

***Internal Cyber Recommendations***

The following recommendations form a solid basis for any security program, and are consistent with the SEC's proposed rules.

*A Written Cyber Risk Assessment*

This report categorizes and prioritizes cyber risk based on an inventory of the information systems' components, including the type of information residing on the network and the potential impact of a cybersecurity incident on the advisers or funds.

The risk assessment should identify service providers to the advisers or funds, identify the information the providers have access to on the network, and any associated risks.

The assessment should also inform senior officers of the advisers or funds "of the risks specific to the firm and ... [identify] cybersecurity threats to information systems that, if compromised, could result in significant cybersecurity events" for the entity.

*Cyber Vulnerability Assessment*

Though not in the proposed rules, in addition to a cyber risk assessment, we recommend clients perform a cybersecurity vulnerability assessment to assess threats and vulnerabilities; determine deviations from acceptable configurations, enterprise or local policy; assess the level of risk; and develop and/or recommend appropriate mitigation countermeasures in both operational and nonoperational situations.

This is one level deeper than the overall cyber risk assessment.

*Identity and Access Management Policy*

Given that perimeter defenses have been shown to be easily breached by attackers, the SEC suggests that cybersecurity risk management rules include "controls designed to minimize user-related risks and prevent the unauthorized access to information and systems."

Under the SEC's proposed rules, registered investment adviser and fund policies and procedures must:

- Require "standards of behavior for individuals authorized to access adviser or fund information systems and any adviser or fund information residing therein, such as an acceptable use policy";

- Identify and authenticate "individual users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification";

- Establish "procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication";

- Restrict "access to specific adviser or fund information systems or components thereof and adviser or fund information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the adviser or fund"; and

- Secure "remote access technologies used to interface with adviser or fund information systems."

The rule also states:

> The proposed cybersecurity risk management rules would require advisers and funds, as part of their cybersecurity programs, to address user access controls to restrict system and data access to authorized users. Such controls are necessary to prevent and detect unauthorized access to systems or client or investor data or information.

In sum, access to an adviser or fund's

> systems and data can be controlled through a variety of means, including, but not limited to, the issuance of user credentials, digital rights management with respect to proprietary hardware and copyrighted software, authentication and authorization methods (e.g., multi-factor authentication and geolocation), and tiered access to

> sensitive information and network resources. Effective controls would also generally include user security and access measures that are regularly monitored not only to provide access to authorized users, but also to remove access for users [who] are no longer authorized, whether due to removal from a project or termination of employment.

*Vendor Supply Chain Risk Management Program*

The proposed rule states, as part of any

> reasonably designed cybersecurity policies and procedures, an adviser or fund would be required to oversee any [third parties and] service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access their information systems and any information residing therein. Advisers and funds would be required to document that [they are] requiring such service providers, pursuant to a written contract, to implement and maintain appropriate [cybersecurity] measures, including measures similar to the elements advisers and fund must address in their own cybersecurity policies and procedures.

Additionally, "[s]uch policies and procedures ... should also include other oversight measures, such as ... periodic contract review processes" and audit rights that allow funds and advisers to ensure that third parties and service providers properly "protect fund and adviser information and systems" — "e.g., notifying the adviser or fund of cybersecurity incidents that adversely affect an adviser's or fund's information, systems, or operations."

*Cybersecurity Incident Response and Recovery Policy/Mandatory Reporting to the SEC*

Registered investment advisers and funds should have the basics in writing, including an incident response plan that defines how the adviser or fund will respond to and recover from a cybersecurity incident.

The incident response plan establishes the incident response team leader and the team participants; accounts for external and internal cybersecurity incident information sharing; and provides criteria for elevating critical information to the C-suite and the board of directors, and for the reporting of significant cybersecurity incidents to the SEC and to clients and investors.

Additionally, "the proposed rules would require advisers and funds to prepare written documentation of any cybersecurity incident, including their response and recovery from such an incident."

*Business Continuity Plan*

The SEC is focused on operational resilience, i.e., the ability to recover from a cyberattack:

In general, an adviser's or fund's cybersecurity program should be designed to reasonably ensure its continued operations when confronted with a cybersecurity incident, whether targeted at the adviser or at a service provider, and maintain access to adviser's or fund's information.

"The ability to recover critical systems or technologies, including those provided by [third parties and] service providers, in a timeframe that meets business" needs is important to mitigating the consequences of cybersecurity incidents.

The rules state, "An adviser or fund may consider implementing safeguards, such as backing up data" — segmented and offline to protect from ransomware attacks — "which can help facilitate a prompt recovery" from a cybersecurity incident.

*Tabletops*

Incident response plans and business continuity plans should not sit on a shelf gathering dust. Plans should be regularly tested and reviewed in tabletop exercises.

Cybersecurity incidents are inherently intense for a relatively short period of time, often a week or two. Given the need to be on top of the incident immediately it is important that each employee, director and officer know his or her role at the outset.

*Annual Report*

The SEC's "proposed cybersecurity risk management rules would require advisers and funds to review their cybersecurity policies and procedures no less frequently than annually."

At least once a year, advisers and funds must:

> (1) review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk over the time period covered by the review; and (2) prepare a written report. The report would, at a minimum, describe the annual review, assessment, and any control tests performed, explain the results thereof, document any cybersecurity incident that occurred since the date of the last report, and discuss any material changes to the policies and procedures since the date of the last report.

*Board Oversight*

Given the importance of good cybersecurity to funds, advisers and investors, the SEC will require the fund's board of directors, including a majority of the independent board, to approve the fund's cybersecurity policies and procedures, as well as any reports on cybersecurity incidents, in order to fulfill the board's oversight duties and to provide accountability for the program.

**Are Public Companies Next?**

The SEC has now proposed the cybersecurity reporting standard for registered investment advisers and funds. It is anticipated that these proposed rules will be enacted in a form similar to what we described above.

Given the SEC's continuing concerns about the individual investor, and given the fact that the cybersecurity and ransomware crisis in the U.S. is not going away anytime soon, the SEC may focus next on similar rules for public companies.

Notably, however, for companies that have already adopted the National Institute of Standards and Technology's cybersecurity framework, in whole or in part, any proposed new rules by the SEC should not change much.

Indeed, a "lean forward" cybersecurity posture under the guidance of the NIST framework would already incorporate many of the SEC's proposed rules. They would be second nature

to these companies.

However, for many companies that have felt that NIST framework measures were unnecessary given the low-stakes nature of their business from a data perspective, conforming to any new SEC rules would require time and effort, as well as board involvement. But our experience shows that it is better to prepare for a cyberattack beforehand than to face a cyber incident unprepared.

---

*Paul A. Ferrillo, Tracee E. Davis and Daphne Morduchowitz are partners at Seyfarth Shaw LLP.*



[1] See SEC Proposed Cybersecurity Risk Management Rules and Amendments for registered investment advisers, available at https://www.sec.gov/news/statement/gensler-statement-cybersecurity-reforms-020922#. The proposed rules are not final at the moment. They are out for a 60-day comment period.

[2] See proposed rule, available at https://www.sec.gov/rules/proposed/2022/33-11028.pdf.

[3] Id.