Hedge Fund Law Report
An Acuris company

hflawreport.com

March 24, 2022

CYBERSECURITY

SEC Proposes Cyber Risk Management Rules for Advisers

By Vincent Pitaro, *Hedge Fund Law Report*

This year, the SEC under Chair Gary Gensler has been on a rulemaking tear. The regulator's growing focus on the size and influence of the private funds industry has now intersected with its longstanding focus on cybersecurity. To that end, the SEC recently proposed sweeping new cybersecurity rules for investment advisers and registered investment funds that would require them to adopt and implement comprehensive cybersecurity policies and procedures; report certain significant cybersecurity incidents to the SEC within 48 hours of discovery; and provide enhanced disclosure about cybersecurity risks and incidents.

"Cyber risk relates to each part of the SEC's three-part mission, and in particular to our goals of protecting investors and maintaining orderly markets," said Gensler in the press release announcing the rule proposal (Proposal). "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," he added.

This article details the proposed rules as they apply to registered investment advisers, with commentary from Avi Gesser, partner at Debevoise & Plimpton, and Clifford E. Kirsch, partner at Eversheds Sutherland.

See "Six Takeaways From the SEC's FY 2021 Enforcement Results" (Jan. 27, 2022); "Recent Experiences With SEC Examinations and Enforcement: Cybersecurity, BCPs, Branch Offices and Disclosures (Part One of Two)" (Dec. 9, 2021); and "Fireside Chat With SEC Chair Gensler: Three Key Disclosure Areas (Part One of Two)" (Nov. 18, 2021).

Rationale for Proposal and Regulatory Framework

Three Primary Justifications

1) Maintaining Operational Capability

Many advisers and funds lack sufficient cybersecurity preparedness, which puts funds and investors at risk, according to the SEC. The Proposal discusses advisers' and funds' growing reliance on technology, the interconnectedness of that technology and the growing sophistication of cyber threats, which could:

- harm clients and investors;
- prevent an adviser or fund from executing an investment strategy;
- prevent clients and investors from accessing their accounts; and
- result in loss of client or investor intellectual property; confidential or proprietary information; or other assets.

Cyber incidents could subject advisers and funds to substantial remediation costs, increases in insurance premiums, private litigation, regulatory action and reputational damage, any or all of which could cause investors to lose confidence in an adviser or the broader financial markets, the SEC cautioned. Therefore, the SEC desires "to promote a more comprehensive framework to address cybersecurity risks for advisers and funds, thereby reducing the risk that advisers and funds would not be able to maintain critical operational capability when confronted with a significant cybersecurity incident," according to the Proposal.

2) Providing Better Information to Investors

The Proposal notes that the SEC is also "concerned that clients may not be receiving sufficient cybersecurity-related information, particularly with respect to cybersecurity incidents, to assess the operational risk at a firm or the effects of an incident to help ensure they are making informed investment decisions."

3) Providing Better Information to the SEC

The SEC seeks "better information with which to conduct comprehensive monitoring and oversight of ever-evolving cybersecurity risks and incidents affecting advisers and funds," according to the Proposal. Reporting of certain cybersecurity incidents will enable the SEC to learn the nature and extent of those incidents, how advisers are responding to them and the implications for investors and the broader financial markets.

Regulatory Framework

The Proposal outlines the relevant regulatory framework for the new requirements, which includes:

- an adviser's fiduciary duty under the Investment Advisers Act of 1940 (Advisers Act) to mitigate risk to clients from the adviser's inability to provide advisory services;
- Rule 206(4)-7 under the Advisers Act, known as the "compliance rule," which requires an adviser to adopt and implement written policies and procedures reasonably designed to prevent violation of the Advisers Act and the rules thereunder by the adviser and its supervised persons;
- Section 248.30 of Regulation S-P, which requires advisers and other SEC-registered entities to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information"; and
- Regulation S-ID, which requires advisers to develop and implement an identity theft prevention program.

The Proposal includes three principal components:

- New Rule 206(4)-9 under the Advisers Act would require advisers to adopt and implement cybersecurity policies and procedures.
- Advisers would be required to notify the SEC of "significant cybersecurity incidents" within 24 hours.
- Amendments to advisers' Forms ADV would require disclosures concerning cybersecurity risks and incidents.

See our two-part series on SEC cybersecurity disclosure enforcement: "Recent Developments" (Oct. 7, 2021); and "Best Practices" (Oct. 14, 2021).

The sweeping new rules would have a significant impact on advisers, Kirsch observed. "As a practical matter, if adopted, advisers would be required to implement extensive new programs with respect to cybersecurity," he said.

Advisers' preparedness varies greatly, Gesser noted. Some already have policies and procedures and incident response protocols that would meet the proposed requirements, but others do not. Moreover, "some have very good polices on paper but haven't tested the policies or are not really following them," he added.

Cybersecurity has been an SEC examination priority for several years, and the Proposal follows recent pronouncements by the SEC staff, Kirsch observed. Although the requirement for advisers to have appropriate policies and procedures suggests a measured approach, the Proposal goes further and could be seen as requiring "a cyber culture or cyber regime at advisers," he said. The most impactful aspect of the Proposal "would cause cybersecurity to be fully integrated into an adviser's compliance, disclosure and governance oversight programs – and to be fully part of an adviser's day-to-day operations and business," he added.

"The [Proposal] would create significant new cybersecurity obligations for private fund advisers," according to Gesser. "Although [the Proposal] states that 'there is not a one-size-fits-all approach,' it contains several required elements, including risk assessment; standards for user security and access; information protection; threat and vulnerability management; and cybersecurity incident response and recovery, as well as heightened disclosure and recordkeeping obligations," he noted.

Although the requirements are extensive, the Proposal does not break much new ground, Gesser continued. The proposed regulations reflect "best practices that cybersecurity experts have recommended for some time and are consistent with the [New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies (Part 500 Regulations)] and the SEC's expectations on the broker-dealer side, as reflected in its Regulation S-P guidance," he explained.

Gensler has emphasized both cybersecurity and increased scrutiny of private funds, Gesser noted. "Targeting policy violations has been a longstanding enforcement approach for the SEC in the registered investment adviser context, and the proposed rules provide a clear 'hook' for doing so in the SEC's priority area of cybersecurity," he observed.

Cybersecurity Policies and Procedures

Mandatory Policies and Procedures

Proposed Rule 206(4)-9 would make it unlawful for a registered adviser to provide investment advice to clients unless the adviser "adopts and implements written policies and procedures that are reasonably designed to address the adviser's cybersecurity risks. . . ."

See "Tailoring a Compliance Program: Why Fund Managers Should Customize (Part One of Three)" (Jul. 16, 2020); and "How Fund Managers Should Structure Their Cybersecurity Programs: Background and Best Practices (Part One of Three)" (Mar. 22, 2018).

Annual Review and Report

Under the Proposal, an adviser would be required to review its cybersecurity policies and procedures at least annually to ensure that they reflect evolving risks. The adviser would also be required to document that review in a written report that:

- describes the review and testing;
- documents any cyber incidents since the last report; and
- discusses any material changes to its policies and procedures.

The report would need to be prepared by the individuals who administer the adviser's cyber policies, "but additional adviser or fund personnel generally should also participate to provide their organizational perspective, as well as ensure accountability and appropriate resources," the SEC advised.

See "Risk Alert on Compliance: Inadequate Annual Reviews, Poorly Implemented Policies and Other Key Takeaways (Part Two of Two)" (Feb. 25, 2021); and "Tailoring a Compliance Program: When Fund Managers Should Review and Update (Part Three of Three)" (Jul. 30, 2020).

Governance and Oversight

Proposed Rule 206(4)-9 rule is intended to give advisers flexibility in managing cyber risks, according to the Proposal. It states that advisers may administer their cybersecurity duties in-house, including as part of a larger company structure, provided they have the requisite "knowledge and expertise." They may also use third parties "subject to appropriate oversight." In either case, those responsible for cybersecurity must be empowered "to make decisions and escalate issues to senior officers as necessary for the administrator to carry out the role effectively." Thus, policies should include clear assignments of roles and duties, as well as reporting lines.

See "How Fund Managers Should Structure Their Cybersecurity Programs: Stakeholder Communication, Outsourcing, Co-Sourcing and Managing Third Parties (Part Three of Three)" (Apr. 12, 2018); and "How Fund Managers Should Structure Their Cybersecurity Programs: CISO Hiring, Governance Structures and the Role of the CCO (Part Two of Three)" (Apr. 5, 2018).

Required Areas

Cybersecurity policies and procedures would be required to address the following five areas.

1) Risk Assessment

An adviser would be required to conduct periodic risk assessments of its information systems and the information it holds, as well as maintain documentation of those assessments. The assessments would need to:

- categorize and prioritize risks based on an inventory of the adviser's systems and information; and
- identify service providers that process or have access to adviser information and assess the cyber risks associated with using those services.

See "How Managers Can Identify and Manage Cybersecurity Risks Posed by Third-Party Service Providers" (Jul. 27, 2017).

A proper risk assessment is a critical prerequisite to developing appropriate cybersecurity policies and procedures, the SEC observed in the Proposal. Assessments of service providers

should consider whether a cyber incident could result in unauthorized access to, or use of, adviser information or adversely affect the adviser's operations or its ability to comply with regulatory obligations. Advisers should consider identifying alternative service providers to take the place of a service provider affected by a cyber incident.

See "Tailoring a Compliance Program: What Fund Managers Should Consider (Part Two of Three)" (Jul. 23, 2020); and "Use a Risk Assessment Template to Take a Thoughtful Approach to Compliance" (Apr. 23, 2020).

2) User Security and Access

The adviser would need controls "designed to minimize user-related risks and prevent unauthorized access to adviser information systems and adviser information," including:

- standards of behavior for access, such as acceptable use policies;
- identification processes, including two-factor authentication;
- password-management protocols;
- access limited to individuals who need it to perform their jobs; and
- secured remote-access technologies.

That process entails developing a clear understanding of who has a legitimate need for access to systems or information, the SEC noted. Those measures should also cover client and investor access to information. In addition, the Proposal discusses the "unique vulnerabilities" associated with mobile devices and encourages advisers to "consider cybersecurity best practices in remote or telework locations."

See our two-part series on digital identity management in a post-pandemic world: "SolarWinds, Zero Trust and the Challenges Ahead" (Apr. 8, 2021); and "A Framework for Identity-Centric Cybersecurity" (Apr. 15, 2021); as well as our two-part series "The Challenges and Benefits of Multi-Factor Authentication in the Financial Sector": Part One (Nov. 2, 2017); and Part Two (Nov. 9, 2017).

3) Information Protection

An adviser would be required to monitor its information systems and protect them from unauthorized use. Periodic assessments would have to cover:

- the sensitivity and importance of information to the adviser's operations;
- whether the adviser holds personal information (PI);
- where and how information is stored and transmitted; and monitoring of information being transmitted;
- access controls and malware protection; and
- the potential impact of a cyber incident on the adviser's operations and ability to provide investment advice.

An adviser would also have to oversee each service provider that holds or processes adviser information. That element includes having a written contract that requires the service provider to "implement and maintain appropriate measures" to protect the adviser's information, including the five measures discussed in the proposed rule.

"Appropriate methods for preventing the unauthorized use of data may differ depending on circumstances specific to an adviser or fund, such as the systems used, the relationship with service providers, or level of access granted to employees or contractors," observes the Proposal.

See "How Do You Put a System of Privacy and Security Controls in Place When Your Target Keeps Moving?" (Jul. 22, 2021); as well as our two-part series on drafting data privacy and security provisions in vendor agreements: "Assessing the Risks" (Apr. 1, 2021); and "Negotiating Critical Provisions and Responding to Incidents" (Apr. 8, 2021).

4) Threat and Vulnerability Management

An adviser's policies would need to "[r]equire measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to adviser information systems and the adviser information residing therein."

The SEC expects advisers to conduct ongoing monitoring, including vulnerability assessments and monitoring of threat information provided by industry and government sources. Mitigation measures may include patch management protocols; processes for tracking and reporting vulnerabilities; accountability for these duties; and role-specific cybersecurity threat, vulnerability and response training.

See "Six Ways for Fund Managers to Prepare for the SEC's Focus on Cybersecurity and Resiliency" (Apr. 30, 2020); as well as our two-part series "K&L Gates-IAA Panel Addresses Regulatory Compliance and Practical Elements of Cybersecurity Testing": Part One (May 21, 2015); and Part Two (May 28, 2015).

5) Incident Response

Adviser policies would have to require measures to detect, respond to and recover from a cyber incident and ensure:

- continued operations of the adviser;
- protection of adviser systems and information;
- internal and external cyber incident information sharing; and
- reporting of significant cyber incidents, per the Proposal.

"We believe it is critical for advisers and funds to focus on operational capability, including resiliency and capacity of information systems, so that they can continue to provide services to their clients and investors when facing disruptions resulting from cybersecurity incidents," the SEC stressed. An incident response plan should designate the specific individuals responsible for effecting each component of the plan and include a "clear escalation protocol."

See our two-part series "Strategies and Tactics for Developing an Effective Tabletop Exercise": Part One (Sep. 19, 2019); and Part Two (Sep. 26, 2019); as well as "How Fund Managers Can Establish Effective Incident Response Plans" (Jul. 18, 2019).

Mandatory Reporting of "Significant" Cybersecurity Incidents

Proposed Advisers Act Rule 204-6 would require an adviser to report to the SEC any "significant adviser cybersecurity incident" or "significant fund cybersecurity incident"

no later than 48 hours "after having a reasonable basis to conclude that any such incident has occurred or is occurring." The proposed rule contains a two-prong definition of "significant adviser cybersecurity incident" – it is a cybersecurity incident, or a group of related cybersecurity incidents, that:

1. significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations; or
2. leads to the unauthorized access or use of adviser information, when the unauthorized access or use of such information results in: (1) substantial harm to the adviser; or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed.

In Gesser's view, this reporting requirement will likely be the most onerous element of the Proposal. "Many firms find short breach notification deadlines, such as 72 hours under the [Part 500 Regulations and the E.U. General Data Protection Regulation], quite difficult to meet," he explained. Thus, "advisers to private funds should start planning to make sure that they can comply with this reporting requirement," he recommended. "The clock starts as soon as there is a 'reasonable basis to conclude' that a significant incident has or is occurring," Kirsch noted.

Form ADV-C

Advisers would report covered incidents on new Form ADV-C, which would be submitted through the Investment Adviser Registration Depository. Form ADV-C would include:

- basic identifying information about an adviser;
- the approximate date of the incident and when it was discovered;
- whether law enforcement has been notified;
- substantive information about the nature and scope of the incident and the adviser's recovery efforts, including whether:
  - any data or PI was stolen;
  - clients or investors have been notified;
  - the adviser's systems or services have been affected; and
  - the incident is the result of an incident at a service provider; and
- whether the incident is covered by insurance.

An adviser would be required to amend Form ADV-C within 48 hours:

- when material in a previously filed Form ADV-C has become materially inaccurate;
- if the adviser discovers new material information about the incident; and
- after resolution of the incident.

The SEC acknowledged that advisers will be required to report at a time when they are under considerable stress from the incident. Nevertheless, the SEC argued "that advisers should have sufficient information to respond to the proposed questions by the time the filing is due to the Commission." Moreover, they would only be required to report what they know at the time of the filing. The SEC's preliminary view is that information reported on Form ADV-C should be confidential.

Cybersecurity Risk and Incident Disclosures

The SEC proposes to add a new Item 20 to Form ADV Part 2A that would require disclosure of:

- the cybersecurity risks that could materially affect the offered advisory services, with a description of how the adviser assesses, prioritizes and addresses the cybersecurity risks created by the nature and scope of its business; and
- any cybersecurity incident that that has occurred within the last two fiscal years that significantly disrupted or degraded the adviser's ability to maintain critical operations, or led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or its clients, including:
    - the affected entities;
    - when the incident was occurred and whether it is ongoing;
    - whether data was stolen or accessed, altered or used without authorization;
    - the impact of the incident on the adviser's operations; and
    - whether the adviser has remediated or is remediating the issue.

A proposed amendment to Advisers Act Rule 204-3(b) would require advisers to deliver interim brochure amendments promptly to existing clients if the amendment discloses a cybersecurity incident or materially amends a previously disclosed incident.

See our two-part series "Lessons Learned From How Advisers Dealt With the October 2017 Amendments to Form ADV": Part One (Feb. 7, 2019); and Part Two (Feb. 14, 2019).

Recordkeeping

The SEC proposes amending Advisers Act Rule 204-2 to require an adviser to maintain, for five years, a copy of all:

- cybersecurity policies and procedures adopted pursuant to Rule 206(4)-9;
- reports documenting annual cybersecurity reviews;
- Form ADV-C amendments;
- reports documenting cybersecurity incidents and responses; and
- reports documenting cybersecurity risk assessments.

See our two-part roadmap to maintaining books and records: "Compliance With Applicable Regulations" (Nov. 2, 2017); and "Document Retention and SEC Expectations" (Nov. 9, 2017).

Requests for Comments

Comments on the Proposal should be submitted by April 11, 2022, or the date that is 30 days after the Proposal is published in the Federal Register, whichever is later. As the Proposal was published in the Federal Register on March 9, 2022, the deadline for comments is April 11, 2022.

Per the SEC's rulemaking practice, the agency is soliciting comments on the following issues:

- whether certain types of advisers or funds should be exempt from the rules;
- whether some or all of the requirements should be scaled to the size of the adviser or fund;
- the appropriateness and clarity of the proposed risk management rules, including how specific they should be with respect to cybersecurity measures, responsible individuals, incident response and other matters;
- current practices regarding mobile devices, monitoring and assessments;
- third-party service providers, including risk management, oversight, insurance and access to information;
- the appropriateness and scope of the annual review and report;
- the appropriateness of the requirement for fund board approval and review of policies and procedures and annual reports;
- the appropriateness of the recordkeeping requirements;
- the appropriateness of the cyber incident reporting requirement, including its scope, reporting timeframe, clarity of definitions, reporting thresholds, interplay with Form PF reporting and amendment requirements;
- the content, filing process and confidentiality of Form ADV-C;
- whether the proposed disclosures would be helpful to investors;
- whether certain funds should be exempt from the prospectus disclosure requirements; and
- whether more specific guidance from the SEC is needed.