Deloitte.

SEC issues cyber rule proposal for advisers and funds

On February 9, 2022, the Securities and Exchange Commission (SEC) proposed cybersecurity risk management rules applicable to registered investment advisers ("advisers"), registered investment companies, and business development companies (collectively, "funds"). With the proposal, the SEC is launching a new chapter in its regulatory approach to cybersecurity.[1] Commissioner Gensler indicated that he has requested the staff of the SEC to develop similar[2] proposals for broker-dealers under Regulation Systems Compliance and Integrity (Regulation S-P).

The regulatory context

The SEC and its staff has signaled increasing scrutiny of cyber practices for some time. The SEC's focus on cybersecurity has extended for years and has geared particular attention to "market systems, customer data protection, disclosure of material cybersecurity risks and incidents, and compliance with legal and regulatory obligations under federal securities laws."[3] Over the past decade, there have been multiple risk alerts as well.[4] In addition, in 2020, the Division of Examinations (previously known as the Office of Compliance Inspections and Examinations) ("Examinations Division") issued a report on cybersecurity and resiliency observations at the beginning of 2020, which was based on observations from "thousands of examinations of broker-dealers, investment advisers, clearing agencies, national securities exchanges and other SEC registrants."[5] Nevertheless, the SEC staff makes clear in the Proposing Release that it continues to observe a lack of cybersecurity preparedness by advisers and funds, which puts clients and investors at risk in the staff's view.[6] The SEC staff goes on to clarify that the existing legal and regulatory framework applicable to advisers and funds is sufficient to encompass business disruptions from cybersecurity incidents as well as customer privacy and third-party oversight considerations.[7] With this background, it is not surprising that a large component of the requirements of the proposed rules under the Proposing Release are captured as leading practices in the 2020 Examinations Report.

SEC cybersecurity evolution (2017–present)

Risk alert: Observations from cybersecurity examinations

OCIE publishes a risk alert to highlight for firms the risks and issues that staff identified during examinations of broker-dealers, investment advisers, and investment companies regarding cybersecurity preparedness.

In addition, the risk alert describes factors that firms may consider to: (1) assess their supervisory, compliance, and/or other risk management systems related to cybersecurity risks, and (2) make any changes, as may be appropriate, to address or strengthen such systems.

OCIE cybersecurity and resiliency observations 2020

Developed through its examinations of thousands of broker-dealers, investment advisers, clearing agencies, national securities exchanges, and other SEC registrants, the OCIE provides observations to assist market participants in their consideration of how to enhance cybersecurity preparedness and operational resiliency.

Exam priorities

OCIE continues to prioritize cyber and other information security risks across the entire examination program.

Risk alerts

OCIE publishes three cybersecurity-related risk alerts, one on ransomware (July), another on safeguarding client accounts (September), and a third related to advisers' compliance programs (November).

Exam priorities

2021 examination priorities include cybersecurity and resiliency, cyberthreat management, and incident response, among other things.

SEC announces three actions charging deficient cybersecurity procedures

SEC sanctions eight firms for violation of Rule 30(a) of Regulation S-P, also known as the Safeguards Rule, which is designed to protect confidential customer information; Section 206(4) of the Advisers Act; and Rule 206(4)-7 in connection with their breach notifications to clients.

SEC proposes cybersecurity risk management rules and amendments for registered investment advisers and funds

SEC proposes rules related to cybersecurity risk management for registered investment advisers, registered investment companies, and business development companies (funds), as well as amendments to certain rules that govern investment adviser and fund disclosures.

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.

The SEC's Division of Enforcement has also prioritized weaknesses in cyber-related practices and has brought enforcement actions over the years. Although the SEC created an enforcement unit focused exclusively on cybersecurity in 2017,[8] it brought its first cybersecurity-related enforcement action in 2014.[9] In 2021 alone, the SEC sanctioned eight firms in three actions related to their cybersecurity practices.[10] Each of the actions pertained to cyber incidents that resulted in the exposure of client personally identifiable information (PII). The firms—a combination of broker-dealers and investment managers—either had not followed their own policies or had failed to implement written policies and were required to pay between $200,000 and $300,000 to settle the charges.

Coinciding with this groundswell of activity at the SEC staff level, the SEC is helmed by a highly ambitious leader in Chairman Gensler, and the Commission has approved each of the proposals put forth by the staff this year.[11]

Summary of the rule proposal

The SEC is proposing new rules and amendments under both the Advisers Act of 1940 (the "Advisers Act") and the Investment Company Act of 1940 (the "Investment Company Act"). Under the Advisers Act, the SEC is proposing: (a) new rules 206(4)-9 and 204-6, (b) amendments to rules 204-2 and 204-3(b), and (c) new Form ADV-C and amendments to Form ADV. Under the Investment Company Act, the SEC is proposing new rule 38a-2 and amendments to Forms N-2, N-3, N-4, N-6, N-8B-2, and S-6.

In totality, the proposal has four major components:

1. Funds and advisers would be required to implement cyber risk management policies and procedures.
2. Advisers would be required to report significant cyber incidents, including significant incidents to the Commission within 48 hours on new Form ADV-C.
3. Advisers and funds would be required to disclose cybersecurity risks and incidents to their investors and other market participants.
4. Advisers and funds would be required to maintain cybersecurity-related books and records.

Policies and procedures

Proposed new rules 206(4)-9 under the Advisers Act and 38a-2 under the Investment Company Act would require firms to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks. The proposal describes five "general elements" of cybersecurity policies and procedures that would be required:

A. **Risk assessment:** Firms would be required to perform periodic assessments of cybersecurity risks associated with adviser/fund information systems and adviser/fund information residing therein and produce written documentation of such risk assessments. This would mean that registrants need to implement risk management programs to continually assess, prioritize, treat, and document risks associated with their information systems on a periodic basis. In addition, firms will need to take a proactive role in sharing and understanding emerging risks from industry/critical infrastructure groups, such as Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to strengthen industry stance and identify new risks. Specifically, firms will need to:

   i. Establish an inventory of information systems (and information residing therein) and implement a well-rounded approach (that considers factors such as information handled, impact of cybersecurity-related incidents involving these systems to advisers/funds, etc.) to categorize and prioritize cybersecurity risks associated with these information systems.

   ii. Implement a third-party risk management (TPRM) program to establish an inventory of third parties or service providers with access to adviser or fund information or information systems and determine whether the firm's third-party risk, compliance, and performance (response and resiliency) expectations are being met throughout the third-party life cycle. Commitment of third parties in safeguarding adviser or fund information should be ensured via written contracts and agreements during onboarding.

Each of proposed rules 38a-2 and 206(4)-9, would require that advisers and funds, as applicable, review their policies and procedures, at least annually, and produce a written report of the review, which describes the review, the assessment, and any control tests performed; explains their results; and documents any incidents that occurred since the preceding report was issued, as well as any material changes to the policies and procedures since the last report was issued. Such written report must be provided to the funds' boards for their review under proposed rule 38a-2. Proposed rule 38a-2 would also require fund boards, including a majority of independent directors, to initially approve the policies and procedures. In the case of unit investment trusts, the fund's principal underwriter or depositor must approve the policies and procedures and receive the annual written reports.

B. **User security and access:** Firms would need to design and implement identity and access management programs for managing access to assets and information based on roles and entitlements. To this effect, registrants will need to:

   i. Establish guidelines for acceptable use of adviser or fund assets, and guide behavior of individuals authorized to access adviser or fund information systems and any adviser or fund information residing in these systems.

ii. Enforce authentication and authorization for adviser or fund information systems via various methods such as multifactor authentication, password management, identity life cycle management, role-based access controls, etc. Firms would need to implement role life cycle management processes (create, composition review, update, discontinue, etc.) consistently across their information systems.

iii. Secure remote access technologies that are used to interface with adviser or fund information systems such that remote access connections implement authentication, authorization, and encryption controls. Integrate remote access controls with other security capabilities (e.g., network access control [NAC], endpoint security, firewalls, centralized security information and event management [SIEM] solutions, etc.), and implement security monitoring and detection capabilities to identify threats on the network's endpoints.

iv. Establish a security awareness and training program to help users understand their cybersecurity roles and responsibilities. Requisite policies and standards pertaining to mobile device management, secure use of adviser or fund information assets, etc. will need to be disseminated.

Another key aspect of the proposed rules is that advisers and funds would need to consider implementation of external identity and access management, commonly referred to as customer identity and access management (CIAM), from a business-to-business (B2B) and a business-to-customer (B2C) standpoint.

C. Information protection: Funds and advisers would be required to establish data protection programs for secure use, processing, transmission, and storage of their information and review compliance via periodic assessments. These assessments should consider:

- Sensitivity of information
- If the information is personal or confidential in nature
- Where and how the information is accessed, stored, and transmitted
- Security safeguards implemented to protect information, such as malware protection, data access, monitoring, etc.
- The potential impact of a cyber incident, especially on the ability to provide services

Advisers and funds need to safeguard their sensitive data from being disclosed or transmitted by users either by malicious intent or inadvertent mistake. There are various security capabilities that advisers and funds may implement to safeguard such sensitive data. These include, but are not limited to:

i. Logging and monitoring for data access or exfiltration, suspicious activity at the database layer, endpoints, and cloud. Further, monitor for sensitive information loss at the endpoints and through common network channels.

ii. Identify and control access to sensitive data by cloud access security broker (CASB), data loss prevention (DLP), data access governance (determine who owns, uses, and has access to sensitive information), and information rights management (restrict internal and external access to sensitive information, i.e., view, edit, copy, and print).

iii. Data loss prevention by scanning for sensitive information on servers, laptops, desktops, and cloud services. Monitor and implement rules to identify and block the transmission of sensitive data being transferred via sharing in cloud, email, and web, as well as to removable devices, and from being copied or printed.

D. Threat and vulnerability management: The proposal requires advisers and funds to implement threat and vulnerability management programs to monitor, detect, mitigate, and remediate cybersecurity threats and vulnerabilities. The vulnerability management program should have a defined governance model to establish accountability for handling vulnerability reports, and processes for intake, assignment, escalation, remediation, and remediation testing. The threat and vulnerability management programs will need to cover the following components:

i. Vulnerability assessment and penetration testing: Registrants should establish and implement a risk-based plan and approach to test for application, system, and network security vulnerabilities and weaknesses. These assessments could include scans or reviews of internal systems, externally facing systems, new systems, and systems used by advisers' or funds' service providers. Vulnerability scans and penetration tests should be conducted on an ongoing basis with no discernible start/stop point (e.g., based on threat landscape, on demand, etc.), and testing schedules will need to be adjusted based on changes in the firm's threat landscape and internal intelligence from security analytics.

ii. Threat intelligence: Advisers and funds would need to establish threat intelligence capabilities to collect and aggregate threat information from multiple sources and leverage the information to identify new cybersecurity threats and vulnerabilities. Threat intelligence from multiple sources (including industry and government sources) should be evaluated for credibility, relevance, and exposure and updated based on changing threat landscape and internal requirements. Threat intelligence should be used to continuously improve patch and vulnerability review processes.

iii. Patch management: Firms should implement patch management programs to acquire, test, and deploy patches for hardware and software vulnerabilities and maintain a process to track and address vulnerabilities timely.

iv. Threat and vulnerability response training: Advisers and funds would need to establish role-specific cybersecurity threat and vulnerability and response training that includes secure system administration courses for IT professionals,

vulnerability awareness and prevention training for web application developers, and social engineering awareness training for employees and executives.

E. Incident response and recovery: The proposal requires firms to establish incident and crisis response programs to detect, respond to, and recover from cybersecurity incidents and define formal processes for interfacing with the SEC and other external agencies to share incident-related information. The proposed rules also require the creation of written documentation of the response to any cyber incident. This would also mean that firms back up their data per defined schedules and based on business impact analysis and recovery point objective (RPO) requirements.

Advisers and funds would also need to establish incident response plans with detailed roles and responsibilities for relevant stakeholders to allow them to respond in an effective manner during cybersecurity incidents. The plans should have a clear escalation protocol to engage the adviser's and fund's senior officers, including appropriate legal and compliance personnel, and fund's board (as applicable) during cybersecurity incidents. In addition, advisers and funds should test their incident response plans through tabletop or full-scale exercises.

The proposal makes clear that the policies and procedures must demonstrate adequate third-party oversight, including documenting due diligence processes and procedures for periodic contract review "that allow funds to assess whether, and help to ensure that, their agreements with [third-party] service providers contain provisions that require service providers to implement and maintain appropriate measures designed to protect fund and adviser information and systems."[12] For example, appropriate oversight includes inquiring about a service provider's business continuity and disaster recovery protocols. Additionally, advisers and funds would need to document, similar to documentation of their own policies and procedures, the security measures that they are requiring of their service providers, which should be similar to their own measures. Further, the proposal describes elements of a required risk assessment including classifying and prioritizing risks based on an information system's inventory and cataloguing service providers that process or can access adviser or fund information.

Reporting of significant incidents on new Form ADV-C

Proposed new rule 204-6 under the Advisers Act would require registered advisers to report any significant adviser cybersecurity incident or significant fund cybersecurity incident—via a new Form ADV-C within 48 hours after having a reasonable basis to conclude that any such incident has occurred or is occurring. The proposal generally defines a significant cybersecurity incident as a cybersecurity incident, or group of related cybersecurity incidents, "that significantly disrupts or degrades" the fund's or adviser's ability (or the ability of a private fund client of the adviser) to continue critical operations, or results in the unauthorized access or use of fund or adviser information, where the unauthorized access or use of such information results in substantial harm to (1) a fund or an investor whose information was accessed or (2) the adviser, a client, or an investor in a private fund whose information was accessed."[13]

Proposed Form ADV-C would contain basic information about the adviser (e.g., SEC file number, primary operating location, contact information, etc.), critical dates associated with the incident, its current status, basic information about the nature and scope of the incident, whether other government or law enforcement entities have been notified, and whether it may be covered under a cybersecurity insurance policy.

Beyond the initial 48-hour reporting window, firms also would be required to update the form within 48 hours to reflect material new or more accurate information and to file an amendment at the completion of the investigation for an incident.

Enhanced disclosure of cyber incidents

The proposal would amend Form ADV Part 2A for advisers' and funds' registration statements. The proposal amends the Form ADV Part 2A to add a new Item 20 entitled "Cybersecurity Risks and Incidents" where advisers need to describe the cybersecurity risks that could materially affect the advisory services and the cybersecurity incidents occurred. The proposed amendments to Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6 would require the funds to provide the cybersecurity-related disclosures and, per the amendments, to describe any significant fund cybersecurity incidents that occurred in the prior two fiscal years in the funds' registration statements. Finally, the proposed amendment to rule 204-3(b) would require an adviser to deliver interim brochure amendments to existing clients promptly if the adviser adds a disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure about such an incident. These disclosures are required to be made via inline XBRL.

Recordkeeping requirements

For advisers, proposed new recordkeeping requirements under Advisers Act Rule 204-2 would require advisers to retain:

- Five years' worth of cybersecurity policies and procedures
- Copies of the written reports documenting the investment adviser's annual review of its cybersecurity policies and procedures in the last five years
- Copies of all Form ADV-C (and ADV-C amendment) filings in the last five years
- Records documenting the occurrence of any cybersecurity incident occurring in the last five years, including records related to any response and recovery from such an incident
- Five years' worth of cybersecurity risk assessments

For funds, proposed new recordkeeping requirements under Investment Company Act Rule 38a-2 would require funds to retain:

- Five years' worth of cybersecurity policies and procedures in an easily accessible place
- Copies of written cybersecurity reports provided to the fund's board (or unit investment trust's principal underwriter or depositor) for at least five years after the end of the fiscal year in which the reports were provided, with reports from the first two years in an easily accessible place
- Documentation of the annual review of the fund's cybersecurity policies and procedures for at least five years after the end of the fiscal year in which the annual review was conducted, with the first two years in an easily accessible place
- Copies of all reports of significant fund cybersecurity incidents to the Commission under Form ADV-C for at least five years after the provision of the report, with the first two years in an easily accessible place
- Records documenting the occurrence of any cybersecurity incident, including records related to any response and recovery from such incident, for at least five years after the date of the incident, with the first two years in an easily accessible place
- Records documenting the risk assessments for at least five years after the date of the assessment, with the first two years in an easily accessible place

Implications of the proposal

The proposal raises a host of considerations for advisers and funds regarding their cybersecurity practices. Some actions for firms to consider:

- *Elevate the governance of cyber risk management:* The rule proposal will necessitate closer collaboration between CISOs and CCOs. For firms that don't have a board subcommittee dedicated to cybersecurity, now may be a good time to organize one or add to the responsibilities of an existing subcommittee.
- *Conduct a gap assessment of cyber program against leading practices and regulatory expectations:* Firms should conduct a gap assessment to baseline their cybersecurity program maturity and identify improvement areas. Firms that have not already done so should review the areas highlighted in the 2020 Examinations Report , which identifies seven areas of focus for firms, all of which are implicated in the Proposing Release. The gap assessment should also incorporate a mapping of current practices to the existing legal and regulatory framework as described by the SEC staff in the Proposing Release.
- *Accelerate the timeline for enhancing your cyber core:* A minimum baseline of cybersecurity program maturity is essential to manage risks. The specter of regulatory imperative can be a powerful motivator for funding delayed projects.
- *Identify a team with primary responsibility for cyber compliance:* Firms are increasingly adopting specialized and deeply skilled groups to manage cyber risks. The proposal affirmatively states that advisers will have the flexibility to self-identify the group responsible for cybersecurity oversight as it pertains to the rule, which may be a combination of compliance and IT professionals as well as third-party service providers.
- *Conduct tabletop exercises:* Firms should have the ability to handle critical incidents, quickly return to normal operations, and repair damage to the business. To this effect, firms need to review their incident response preparedness by engaging in cyber wargaming and other tabletop exercises to measure the efficacy of their incident and crisis response capabilities.

The proposal does not constitute a final rule, and the SEC has solicited comments, including on whether the changes are too prescriptive (or conversely not prescriptive enough) as currently designed. As with many regulatory proposals, market participants are likely in various states of preparedness. This proposal is an opportunity for firms that are lagging in their cyber practices to step up and accelerate their pace of investment ahead of final regulatory mandates and consequences. Given heightened cyberthreats, advisers' status as fiduciaries, and increasing regulatory expectations, the time is right for firms to elevate their cybersecurity efforts and embrace leading practices as outlined in the 2020 Examinations Report, regardless of whether the proposed rules are implemented as proposed.

Appendix

Table of actions for advisers and funds to consider

Governance and risk management	• Engage senior leaders other than CISO, including CCO and others • Develop a risk assessment model • Adopt and implement written policies and procedures • Test policies and procedures to ensure their effectiveness • Develop internal and external communication plans for a cyber event
User security and access	• Identify and categorize information residing within their systems • Map user access to systems and data • Implement strong password standards and multifactor authentication • Develop policies to limit user access as appropriate, separate duties for access approval, and recertify access on a periodic basis • Monitor user access including failed login attempts and access anomalies
Information protection	• Enact a vulnerability management program to routinely scan for weakness in code, applications, servers, and databases • Control, monitor, and inspect all incoming and outgoing network traffic • Develop capabilities to detect threats on end points • Manage use of mobile devices and implement protection plan
Threat and vulnerability management	• Catalogue vendor relationships and implement a vendor relationship management program • Conduct trainings to increase knowledge and awareness of cyberthreats among staff and leadership
Incident response	• Establish a framework for determining materiality classification for cyber incidents • Develop a plan for escalation and communication, including reporting requirements • Assign key owners of the plan and test it via war games, etc.
Third-party service providers	• Develop a risk assessment model • Establish a framework for determining materiality classification for cyber incidents • Identify and categorize information residing within their systems

Contacts

Maria Gattuso
Principal | Deloitte & Touche LLP
mgattuso@deloitte.com
+1 203 321 7098

Bruce Treff
Managing Director | Deloitte & Touche LLP
btreff@deloitte.com
+1 617 437 3087

Nitin Pandey
Managing Director | Deloitte & Touche LLP
npandey@deloitte.com
+1 212 436 7215

Najeh Adib
Senior Manager | Deloitte & Touche LLP
nadib@deloitte.com
+1 212 436 5750

Meghan Burns
Manager | Deloitte & Touche LLP
megburns@deloitte.com
+1 202 220 2780

Endnotes

1. Securities and Exchange Commission (SEC), "SEC proposes cybersecurity risk management rules and amendments for registered investment advisers and funds," press release 2022-20, February 9, 2022 (the release hereafter referred to as the "Proposing Release").
2. SEC Chair Gary Gensler, "Statement on Proposal for Mandatory Cybersecurity Disclosures," March 9, 2022.
3. SEC, "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," 17 CFR Parts 230, 232, 239, 270, 274, 257, and 279, February 9, 2022.
4. Ibid, p. 7, note 5.
5. SEC Office of Compliance Inspections and Examinations (OCIE), "Cybersecurity and resiliency observations," January 27, 2020 (the "2020 Examinations Report").
6. Ibid, p. 8.
7. Ibid, pp. 9–12.
8. OCIE (n 5, p. 1 [note 1]).
9. SEC, "Crypto Asset and Cyber Enforcement Actions," last modified July 11, 2022.
10. SEC, "SEC announces three actions charging deficient cybersecurity procedures," press release 2021-169, August 30, 2021.
11. On March 9, 2022, the SEC approved a separate rule proposal requiring cyber incident disclosures by all public companies.
12. SEC, "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," 17 CFR Parts 230, 232, 239, 270, 274, 257, and 279, February 9, 2022, p. 27.
13. Ibid, pp. 42–43.

Deloitte.