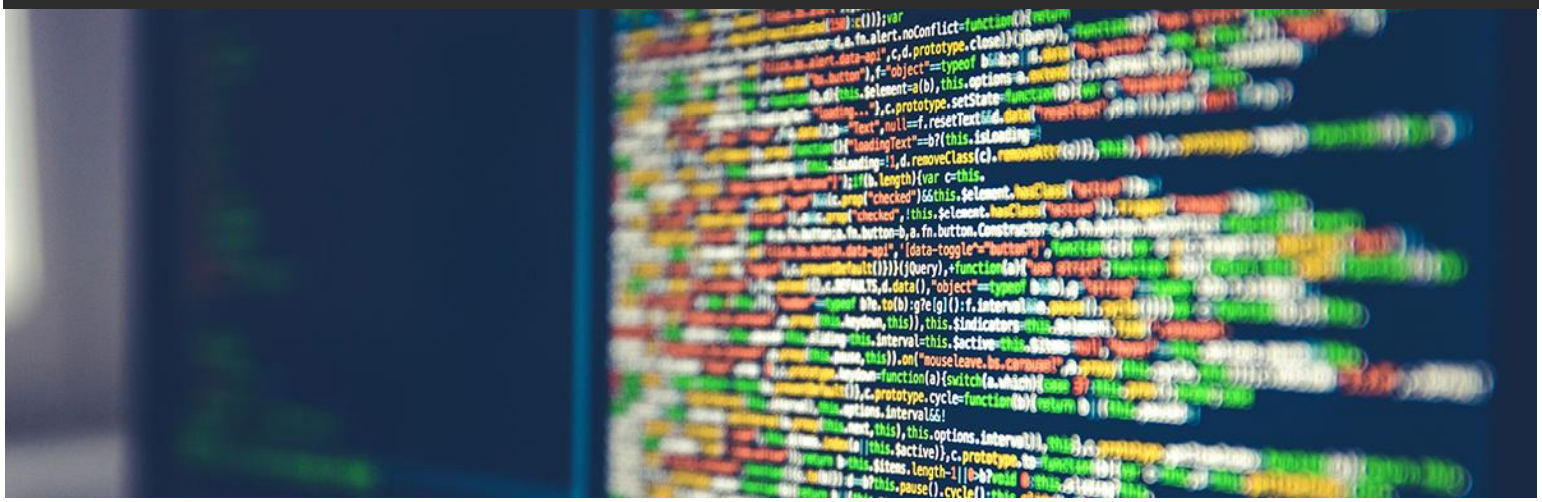
GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity/ Financial Regulatory & Compliance



February 2022

SEC Issues Proposed Cyber Rule, Including 48-Hour Breach Reporting Requirement

This GT Alert covers the following:

- The SEC issued a proposed cybersecurity rule applicable to registered investment advisers and registered investment companies, but did not issue the rule to publicly traded companies.
- The rule requires notification to the Commission within 48 hours of discovering a significant cybersecurity incident.
- The rule also requires extensive policies and procedures, including a written information security plan and incident response plan, to address and respond to cybersecurity threats.
- Companies will be required to increase disclosures and recordkeeping around cybersecurity practices, risks, and incidents.

On Feb. 9, 2022, the SEC released its long-awaited proposed cybersecurity rule, and there's a lot to unpack. As GT reported previously, the SEC increased enforcement of cybersecurity compliance in 2021. As recently as Jan. 24, 2022, Chair Gary Gensler made cybersecurity the focus of his speech at Northwestern Law School's Securities Regulation Institute.

© 2022 Greenberg Traurig, LLP

As an initial matter, the rule only applies to registered investment advisers (RIAs), registered investment companies (RICs) and business development companies (BDCs). To the extent most private funds are advised by RIAs, such funds will also be impacted. Publicly traded companies are mentioned nowhere in the 252-page proposed rule. The public comment period will remain open for 60 days, so it's possible that the text of the rule itself may change between now and when it is finalized.

The proposed rule itself is in line with a number of recent rules from federal agencies attempting to tighten compliance around assessing and addressing cybersecurity risks and requiring regulatory breach reporting within a very short time frame of discovering an incident. The proposed rule addresses four main categories: (1) cybersecurity policies and procedures; (2) cybersecurity disclosures; (3) regulatory reporting of cybersecurity incidents; and (4) recordkeeping of cybersecurity incidents. The new requirements would be substantially similar for both advisers and funds, and the proposed rule would amend applicable regulations pertaining to each. The Commission has recognized that a "one size fits all approach" isn't feasible given the wide variations in size, resources, and sophistication, but it clearly intends to hold all regulated entities accountable for compliance at some level.

Policies & Procedures

The SEC is requiring substantial documentation of an organization's cybersecurity practices. Importantly, the SEC would require the board of directors of a RIC or BDC to initially approve cybersecurity policies and procedures and review reports on cyber incidents and material changes to policies and procedures, noting that "Board oversight should not be a passive activity."

Although a number of state laws have long required companies under their jurisdiction to have a written information security plan, also known as a "WISP", the SEC has made it clear that it must contain some key elements:

(1) **A risk assessment, including assessment of risks associated with certain service providers, oversight of such providers, and appropriate written contracts with such providers**. This comes as no surprise given the interest the SEC has taken in the December 2020 SolarWinds Orion hack, which exposed more than 18,000 companies to a possible security breach attributed to Russian hackers. The SEC recognizes that a company's security is only as good as the weakest link of its vendors.

(2) **User security and access**. The proposed rule would require companies to have an acceptable use policy outlining standards of behavior for individuals with certain access to information and systems, a method for identifying and authenticating individual users, expressly requiring multifactor authentication (MFA); establishing procedures for passwords; restricting access to employees on a "need to know" basis; and securing remote access technologies. The express requirement of MFA mirrors the enforcement actions announced Aug. 30, 2021, in which the SEC took eight registered broker-dealers and investment advisers to task for, among other things, failing to have MFA in place to prevent a compromise of email accounts, exposing sensitive information. Remote access requirements make sense in light of the risk we've seen emerge since the sudden onset of remote work due to COVID-19 beginning in March 2020.

(3) **Information protection**. Organizations will be required to conduct a periodic assessment of their information systems and information residing on such systems. The assessment should then be used to implement measures to prevent unauthorized access or use of data. The SEC gives examples of utilizing encryption, network segmentation, and access controls to reduce risks identified in a security assessment.

© 2022 Greenberg Traurig, LLP

(4) **Cybersecurity threat and vulnerability management**. The proposed rule would require ongoing monitoring of risks and vulnerabilities, including conducting network and applications scans and vulnerability assessments, as well as monitoring publicly available sources for the latest intel on security threats.

(5) **Cybersecurity incident response and recovery**. The SEC also is requiring an incident response plan (IRP) designed to ensure that a company can continue to operate during a significant cyber event, most likely a nod to the massive increase in ransomware attacks. The IRP should also include measures to protect systems and information, report significant events to the Commission, and document a cybersecurity incident, including the response and recovery efforts. The Commission also notes that the IRP should be tested, which generally comes in the form of breach tabletop and business continuity exercises.

Disclosures

Proposed amendments to part 2A for Form ADV and proposed amendments to fund registration statements would require a narrative description of the cybersecurity risks advisers face, how they assess, prioritize, and address cybersecurity risks and any significant adviser or fund cybersecurity incidents that had occurred in the past two years. As a practical matter, this will require that changes in cybersecurity policies as well as recent incidents must be reviewed annually when updating the form ADV and registration statements.

Regulatory Reporting of Cyber Incidents

Probably the biggest proposal that will make regulated entities take notice is the requirement that advisers and funds report significant cybersecurity incidents to the Commission within 48 hours. This is in line with the recent final rule issued by multiple banking regulators containing a 36-hour regulatory breach notification requirement for significant breaches. *See* GT Alert. Like the banking rule, the definition of a reportable breach does not apply to every cyber incident. Instead, reporting is limited to a significant cybersecurity incident that "significantly disrupts or degrades…the ability to maintain critical operations, or leads to the unauthorized access or use of [] information [that] results in substantial harm." The Commission has provided examples of such events, including ransomware, significant monetary or intellectual property loss, or theft of personally identifiable or proprietary information, but only those that "result in substantial harm." Perhaps recognizing that 48 hours is a very short period of time in the world of cyber incidents, the Commission expects only an initial report, with subsequent, more fulsome reports to follow. In practice, reporting on this time frame will be tight, and proper incident response plans and testing of those plans will be critical.

Recordkeeping of Cyber Security Incidents

Under the new recordkeeping requirements, advisers and funds would be required to maintain, for five years, records of: (1) cybersecurity policies and procedures; (2) annual reviews thereof; (3) documents related to the annual reviews; (4) regulatory filings related to cybersecurity incidents required under the proposed amendments; (5) any cybersecurity incident; and (6) cybersecurity risk assessments. The Commission is signaling that it means to hold organizations accountable for maintaining written proof of its compliance with the new proposed rule. Further, it is often easier for the Commission to establish recordkeeping violations than violations of substantive rules.

© 2022 Greenberg Traurig, LLP

Takeaways

Even if the final rule varies from the proposed rule, it is clear the Commission is serious about addressing and enforcing cybersecurity risks. Companies should consider taking the following steps now in anticipation of the impending regulation and likely enforcement:

- Conduct a gap assessment of cybersecurity practices, using the measures identified in the proposed rule as a guide.
- Identify vendors to assist in conducting a cybersecurity risk assessment to identify vulnerabilities that could expose the company to a data breach and address those vulnerabilities.
- Ensure someone within the organization has responsibility for cybersecurity compliance. If it's everyone's job, it's no one's job. At the same time, train each and every employee to identify common threats, such as phishing and social engineering campaigns.
- Prepare an incident response plan that addresses likely business risks from a breach, including legal requirements for notification in light of the 48-hour rule, notifying and keeping stakeholders informed, and ensuring business continuity.
- Conduct a tabletop exercise with your exercise leadership team. The tabletop should walk through the steps of a major cybersecurity attack to create muscle memory for team members to rely on in the event of a real incident.
- Review vendor contracts for security compliance requirements and, where possible, issue a data security addendum to bind the vendor to the same requirements as set forth in the proposed rule. Ensure you have the right to audit the vendor's practices, and consider sending a detailed questionnaire or requiring proof of compliance with a recognized data security standing, like ISO, NIST, or SOC-2.
- Consider whether cyber insurance is appropriate. The cyber insurance market has gotten increasingly stringent in its underwriting, particularly of what it considers "high risk" industries, while increasing the costs of policies. Still, cyber insurance can mitigate substantial losses in the event of a major attack.
- Create procedures to ensure that disclosures required by the proposed rule will be added to annual updates of a Form ADV and fund registration statements.
- Document your practices and steps so you can "show your work" if ever requested by the Commission.

Authors

This GT Alert was prepared by:

- Arthur Don | +1 312.456.8438 | dona@gtlaw.com
- Steven M. Malina | +1 312.476.5133 | malinas@gtlaw.com
- Jena M. Valdetero | +1 312.456.1025 | valdeteroj@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Long Island. Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ¬Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¤Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2022 Greenberg Traurig, LLP. All rights reserved.*