Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

SEC Chair Gensler Warns of a New Era of Cyber-Securities Laws

January 31, 2022

Gary Gensler, Chair of the U.S. Securities and Exchange Commission (SEC), signaled a new era of cybersecurity law (and accompanying enforcement) in his keynote address "Cybersecurity and Securities Laws" on January 24, 2022, at the Northwestern Pritzker School of Law's Annual Securities Regulation Institute. Noting the ever-increasing risk of cyberattacks on the securities markets, Gensler identified new and expanded SEC initiatives and proposals to address those risks. The overall message was clear: under his leadership, the SEC will seek to bolster data privacy and cybersecurity requirements, and to enhance its reporting and disclosure regime for cyber risks and cyber events.

SEC Enforcement Backdrop

Gensler's warning follows the latest series of enforcement actions taken by the SEC relating to alleged cybersecurity failures. Most recently, on August 30, 2021, the SEC settled three separate actions where cloud-based email accounts of individuals who worked at SEC registered entities were taken over by unauthorized third parties, potentially compromising the personally identifying information (PII) of thousands of clients. All three actions were brought against registered investment advisors and settled for six figure penalties. On August 16, 2021, the SEC announced that a London-based public company that provides educational publishing and other services to schools and universities agreed to pay $1 million to settle charges under the antifraud provisions that it misled investors about a 2018 cyber intrusion and had inadequate disclosure controls and procedures. And on June 15, 2021, the SEC announced that a real estate settlement services public company agreed to pay a $487,000 penalty for disclosure controls and procedures violations related to a cybersecurity vulnerability that exposed sensitive customer information.

Gensler's Points of Focus

Gensler began his speech by noting that the economic costs of cyberattacks are estimated in the billions, if not trillions, of dollars and that, increasingly, cyberattacks target the financial sector and securities market. Gensler noted that the financial sector is a target for attacks "[b]ecause that's where the money is," invoking the famous quote from bank robber Willie Sutton. Gensler identified potential new policies and

Contact Information

If you have questions concerning this alert, please contact:

White Collar Investigation and Cybersecurity

Ian P. McGinley
Partner
imcginley@akingump.com
New York
+1 212.872.1047

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Peter I. Altman
Partner
paltman@akingump.com
Los Angeles
+1 310.728.3085

Michael A. Asaro
Partner
masaro@akingump.com
New York
+1 212.872.8100

David Giller
Counsel
dgiller@akingump.com
New York
+1 212.872.8094

initiatives to improve the overall cybersecurity posture and resiliency of entities that fall within the scope of the SEC's jurisdiction, with three main areas of focus: cyber hygiene and preparedness, cyber incident reporting to the government and, in certain circumstances disclosure to the public.

In doing so, Gensler identified three groups of entities that the SEC is focused on: (i) SEC registrants, including broker-dealers, investment companies, registered investment advisers and other market intermediaries; (ii) public companies; and (iii) service providers that work with SEC financial sector registrants but may not be registered with the SEC themselves. Gensler commented at the end of his speech that the SEC is mindful that its own operations are not immune from cyberattack.

SEC Registrants. Gensler announced three cybersecurity projects that SEC staff were working on involving SEC registrants and suggested that these projects could likely be expanded to apply to a broader group of entities.

- First, evaluating the expansion of Regulation Systems Compliance and Integrity ("Reg SCI")—a regulation adopted in 2014 to govern stock exchanges, clearinghouses, alternative trading systems and self-regulatory organizations that fall under SEC jurisdiction—to cover what Gensler referred to as "other large, significant entities," such as the "largest market-makers" and investment companies, investment advisers and broker-dealers. Reg SCI specifically requires the maintenance of appropriate technology programs, business continuity plans and data backups, and the application of the rule to a new set of SEC registrants would mark a significant expansion of its scope. Gensler also noted that at the next Commission meeting the SEC would consider whether to also bring trading platforms for government securities under the scope of Reg SCI. On January 26, following the Commission meeting, the SEC proceeded to propose rules that would apply the systems integrity provisions of Reg SCI to certain alternative trading systems that trade government securities and expand other regulations to cover alternative trading systems that trade government securities, National Market System (NMS) stock and other securities.
- Second, instituting reforms that would cover other financial sector registrants, such as investment companies, investment advisors and broker-dealers, that are currently not covered by Reg SCI, with the goal of reducing the risk that these registrants could not maintain critical operational capability during a significant cybersecurity incident. Gensler noted that while various rules may already implicate these registrants' cybersecurity practices, he has asked his staff to make recommendations around how to strengthen registrants' cybersecurity hygiene and incident reporting.
- Third, evaluating the modernization of Regulation S-P—a regulation enacted two decades ago that requires registered broker-dealers, investment companies and investment advisers to protect customer records and information. Notably, Gensler requested that his staff specifically examine both the substance and timing of notifications to customers in the event of a data breach.

Public Companies. Gensler posited that public companies and their shareholders make a "bargain" with each other—namely, shareholders decide what risks they are willing to take while public companies commit to share information on a regular basis,

Corporate and Corporate Governance

Garrett A. DeVries
Partner
gdevries@akingump.com
Dallas
+1 214.969.2891

Cynthia M. Mabry
Partner
cmabry@akingump.com
Houston
+1 713.220.8130

Cynthia Perez Angell
Senior Practice Attorney
cangell@akingump.com
San Antonio
+1 713.250.2245

including risks arising from cybersecurity. Gensler noted particular areas of focus while discussing this "bargain":

- First, the efficacy and completeness of companies' cybersecurity practices and cyber risk disclosures including cybersecurity governance, strategy and risk management. Gensler stated that all parties would "benefit" if there were a "consistent, comparable, and decision-useful manner" of disclosure.
- Second, whether and how companies should update disclosures following cyberattacks. The SEC's recent penalties against public companies that either failed to disclose cyber incidents or disclosed in a misleading manner stands as a stark reminder that there are risks of violations of both the disclosure control requirements and the antifraud provisions if incidents are handled incorrectly.

Third-Party Service Providers. Gensler also discussed third-party service providers, which are not registered with the SEC, but play a critical role in financial services as registrants increasingly outsource their data services. He noted that these service providers can include "investor reporting systems and providers, middle-office service providers, fund administrators, index providers, custodians, data analytics, trading and order management, and pricing and data services, among others." The result is that service providers' cybersecurity risk affect registered entities. Gensler identified potential remedial measures including requiring certain registrants to identify service provers that could pose a risk to their systems and holding registrants accountable for service providers' cybersecurity measures. He also indicated that it "might be worthwhile" for the SEC and market regulators to be granted greater authority over third-party service providers.

Lessons for Entities That Fall Within the SEC's Jurisdiction

Chair Gensler's speech is yet another warning to all entities that fall within the SEC's jurisdiction that cybersecurity remains integral to the SEC's mission. If the SEC enacts the regulations that Gensler suggested in his speech (and there is every reason to believe it will given the current composition of the Commission), SEC registrants, public companies and perhaps even third-party service providers will have increased obligations to prevent cyberattacks and disclose information related to cyber risk and cyber events. Here are a few takeaways from this speech that all affected entities should be thinking about now to prepare for these potential new regulations.

- The SEC's proposals involve the application of Reg SCI to a new of class of registrants. Gensler noted that the purpose of this expansion is to "shore up the cyber hygiene of important financial entities." As such, all potentially affected entities should evaluate their cybersecurity programs and consider implementation of additional efforts to further cyber hygiene, such as updating software regularly, adopting incident response plans, requiring employee training and mandating complicated passwords and multi-factor authentication to gain access to systems.
- In the area of data privacy, and consistent with the growing regulatory trend to reduce the number of days to notify an individual after discovering a breach, Gensler suggested expanding and modernizing rules for registrants for disclosing data breaches and notifying customers and clients about these breaches. He noted that he was considering altering the "timing and substance" of such notices, which leads to the plausible inference that the SEC believes existing disclosures and

notifications have been late and often lacking in detail. Registrants therefore should evaluate their procedures associated with the timing and substance of their disclosure procedures given the focus on the scope of Reg S-P.

- Gensler also suggested the current disclosures of cyber risks by public companies has been insufficient. Gensler noted that the public would "benefit if this information were presented in a consistent, comparable, and decision-useful manner." Indeed, with the rise in large ransomware attacks and data breaches, such as those last year impacting a wide variety of companies and industries, all public companies would be well advised to revisit the thoroughness and timeliness of their cyber risk disclosures.

Finally, all affected entities should identify and monitor the practices of third-party service providers who maintain investor or client information and are at risk from cyberattack. Gensler's remarks are a recognition that cybersecurity weakness of a third party or contractors often results in a business' data being compromised and inappropriately accessed. For example, in the recent SolarWinds data hack, hackers comprised third-party software, which was used by hundreds of government agencies and businesses. Although outside the SEC's purview, the SEC may investigate registrants' actions with regard to those service providers and hold registrants responsible for their third-party providers' cybersecurity deficiencies.

akingump.com