PLI Chronicle

May 2023

SEC as Cyber Cop

Brian Finch

David Oliwenstein

Pillsbury Winthrop Shaw Pittman LLP

During his first two years as Chair of the Securities and Exchange Commission (SEC), Gary Gensler has led the agency down a path of aggressive enforcement and proposed an ambitious rulemaking agenda. The Chair's unyielding enforcement agenda has resulted in, among other things, record levels of monetary relief and industry sweeps that have significantly impacted behavior of Wall Street.

But when historians write the book on the Gensler-era, we believe that, although the Chair will certainly be remembered for the amount and number of penalties that his staff imposed, the Chair's legacy will ultimately be defined by his initiatives to expand the type of conduct that the SEC polices. A prime example of this is the SEC's efforts to serve as "Cyber Cop" on the Wall Street beat.

The SEC's Existing Authority to Police Cybersecurity

To understand the SEC's efforts to expand its purview regarding cybersecurity, we begin with an overview of the agency's existing authority. First and foremost, the SEC has broad authority under the antifraud provisions of the securities laws to pursue entities—especially public companies—that make material misstatements or omissions regarding cybersecurity. These failures have taken various forms including misleading disclosures about ransomware attacks, misrepresentations about theft of data, and wholesale failures to disclose significant breaches. All three of these cases were charged as negligence-based violations under Section 17(a) of the Securities Act of 1933.

Each of those cases also included an accompanying violation of the SEC's disclosure controls and procedures rules—in essence, these companies failed to devise

and implement policies and procedures that would reasonably ensure that important information about cyber matters was elevated up the corporate ladder so that officers could evaluate whether disclosure was necessary. The SEC also brought a standalone disclosure controls and procedures case (i.e., without an accompanying disclosure failure) against another public company for ignoring credible information from a cybersecurity journalist indicating that the company was the victim of a breach in which extensive and sensitive personal data was exposed.

The SEC has additional tools to pursue cyber-related violations at regulated entities—i.e., broker-dealers, registered investment advisers, investment companies, and securities self-regulatory organizations. In recent years, the SEC has brought enforcement actions against regulated entities for violating the "safeguards rule" of Regulation S-P, which requires firms to adopt and implement policies and procedures to protect customer records and information, including personally identifiable information. In September 2022, the SEC charged an international financial institution for failing to take sufficient precautions to protect customer data on computer hardware that the bank was disposing. One year prior, the SEC announced a sweep against eight broker-dealers and investment advisers for Regulation S-P violations, mostly in relation to failure to consistently deploy multifactor authentication across similar categories of email accounts.

The SEC also has powerful existing tools in its arsenal to punish regulated entities that fail to take appropriate measures to prevent identify theft. Regulation S-ID requires firms to adopt a comprehensive identity theft prevention program. In July 2022, the SEC announced a sweep against broker-dealers and investment advisers that failed to 1) tailor policies and procedures to specific identified risks; 2) identify, detect, and respond appropriately to red flags of identity theft; and 3) regularly update policies to address evolving risks.

These are the hooks upon which the SEC has principally relied to date to police the cybersecurity of the financial markets. Of course, the agency has other well-settled tools in its proverbial toolkit. As a high-profile example, the SEC has brought enforcement against individuals that hack sensitive databases and then misappropriate that stolen data to commit insider trading. And the SEC has charged several entities with violations of Regulation SCI, which imposes an enhanced cyber-regulatory regime on "SCI entities"—i.e., organizations that directly support key securities market functions (e.g., stock and options exchanges, alternative trading systems, certain clearing agencies).

The SEC'S Efforts to Expand Its Authority via Rulemaking

Although the existing framework provides the SEC with many tools to police the cybersecurity of securities market participants, the Gensler-led Commission seems to believe that existing regulations are inadequate. To remedy various perceived gaps, the SEC has proposed a set of sweeping new rules that, if enacted, will overhaul the cybersecurity obligations of public companies and regulated entities. Of course, new rulemaking will almost certainly lead to new enforcement initiatives.

Public Companies. On March 9, 2022, the SEC proposed cybersecurity rules for public companies. These rules, when adopted, will overhaul SEC oversight of issuers' cyber regimes. Although the proposal contains many components, commenters have focused principally on new reporting requirements. Those requirements would mandate public companies to report via a Form 8-K any material cyber incidents within four days of concluding that an incident was material and to provide updates on these incidents in Forms 10-K and 10-Q. Companies will have to consider whether a cyber incident is material based on longstanding principles of materiality and guidance issued by the Commission and its staff in 2018 and 2011. The proposed rules would also require companies to report immaterial incidents that are material in the aggregate.

The SEC's proposal is not limited to disclosure of cybersecurity incidents. The rules would amend Regulation S-K to require companies to describe their policies and procedures for identifying and managing risks from cyber threats, including from third-party service providers. Companies would be required to disclose any cyber event—even those that are entirely immaterial—if the event leads to a policy change.

Finally, the rules would impose various governance obligations. The proposal would require companies to disclose their board of directors' oversight of cyber risks and directors' and officers' expertise in implementing and managing cybersecurity. Companies would have to disclose "any detail necessary to fully describe" the nature of directors' expertise and whether they have a designated chief information officer, and, if so, that officer's relative seniority within the company.

Regulated Entities. On February 9, 2022, the SEC proposed new rules to address purported cyber vulnerabilities for registered investment advisers and funds. The proposed rules would require funds to implement written security policies and procedures, report significant cyber incidents on a new confidential form and adhere to new record-keeping requirements designed to facilitate the Commission's inspection and enforcement capabilities.

Prior to acting on the agency's ambitious 2022 cyber rulemaking proposals, the SEC in March 2023 proposed three additional sets of rules for public comment on top of the pending rulemaking. The first proposal would amend Regulation S-P to require regulated entities to notify victims of data breaches within thirty (30) days. The proposal would also expand the categories of information that are subject to the "safeguards rule" and require firms to implement additional policies and procedures designed to address unauthorized access or use of customer information.

The SEC's second proposal would broadly require regulated entities to implement various cybersecurity-related policies and procedures that are reasonably designed to address all cybersecurity risks. The rule would require firms to reassess the sufficiency of those processes on at least an annual basis. To address the SEC's perceived blind spots into cyber incidents at registrants, the proposal would impose notification requirements on firms that experience significant cybersecurity incidents.

The third component of the SEC's 2023 triumvirate of cyber proposals is an update to Regulation SCI. According to Chair Gensler, this rulemaking is designed to reflect substantial changes to securities trading and associated technology since the SEC first adopted Regulation SCI in 2014. If approved, the rule would expand the types of entities subject to the rule's ambit (SCI entities) to include registered security-based swap data repositories, all clearing agencies that are exempt from registration, and certain large broker-dealers. The proposal would also impose additional reporting requirements by expanding the types of incidents that would trigger notifications to the SEC and create additional recordkeeping requirements for SCI entities. Finally, the rule would require SCI entities to enhance and supplement their existing policies and procedures to cover additional security risks identified by the SEC.

Chair Gensler has made cybersecurity a top regulatory priority, and we expect the SEC to adopt all five of these sets of rules substantially as originally proposed. Once adopted, collectively, these new regulations will provide the SEC staff with a broad mandate to monitor the cybersecurity of thousands of entities. And given the SEC's growing appetite for enforcement in this area, companies must proactively prepare for imminent changes to the cyber-regulatory regime.

The SEC's Efforts to Expand Its Authority Without Rulemaking

The SEC has attempted to expand its authority to regulate the cybersecurity of market participants without engaging in formal rulemaking. In 2018, the SEC issued a report pursuant to Section 21(a) of the Securities Exchange Act of 1934 in which the Commission warned public companies that internal accounting controls should be

tailored to address cybersecurity vulnerabilities. The report was based on the Division of Enforcement's investigation of nine issuers that were victimized by business email compromises. In issuing the report, the SEC essentially declared to the market that the agency has the authority to charge public companies with internal *accounting* controls failures based on perceived lapses in cybersecurity procedures, even though cyber "controls" are facially unrelated to accounting or financial reporting. The SEC has not yet brought a case on this untested theory, but we would not be surprised if they attempted to do so before the expiration of the Gensler era.

The SEC continues to aggressively investigate potential violations of the securities laws in the wake of public company data breaches. Although most other law enforcement agencies would correctly consider companies impacted by breaches to be victims, Chair Gensler considers cybersecurity failures to be an "existential threat" to the financial markets. Consequently, the Chair's staff remains focused on identifying enforcement hooks to hold public companies accountable for any perceived lapses.

Market Participants Should Adopt Proactive Measures to Guard Against the Long Arm of SEC Enforcement

Public Companies. As discussed above, public companies are required to maintain a system of disclosure controls and procedures to ensure that important information is escalated to senior management in a timely manner to enable executives to evaluate potential disclosure obligations. In light of those requirements, as well as the SEC's expectations regarding timing as memorialized in the agency's proposed cybersecurity rulemaking, companies should evaluate their disclosure controls and procedures to assess the adequacy of internal reporting regarding cyber matters.

Because of the lack of substantial guidance regarding the circumstances under which cyber events are material, if a company experiences a significant cybersecurity event, management should evaluate disclosure obligations with the assistance of various constituencies, including legal advisors, auditors, chief information security officers and other security experts. To that end, directors and officers should consider brushing up on evolving cyber risks, and companies should have a designated chief information security officer within their governance structures.

If a company concludes that it is required to make a cyber-related disclosure, it must not downplay the seriousness of the incident. Companies should also be mindful that the SEC will expect them to disclose the following information:

- When the incident was discovered and whether it is ongoing;

- A brief description of the nature and scope of the incident;
- Whether any data was stolen, altered, accessed or used for any other unauthorized purpose;
- The effect of the incident on the registrant's operations; and
- Whether the registrant has remediated or is currently remediating the incident.

Companies should also review their existing disclosures to ensure that they accurately discuss the quality of their cybersecurity controls. Companies that overstate the efficacy of their security risk SEC investigations and enforcement actions.

Finally, companies should review the cybersecurity controls and procedures that their third-party vendors have in place. Many cyber risks that firms face may arise from relationships with third parties (e.g., placement agents, vendors), and the SEC may begin to hold firms accountable for security failures caused by or through these partners. Companies should conduct due diligence on the protections their third-party vendors use, including by reviewing the vendors' cybersecurity policies, obtaining a written commitment from third parties that they will maintain the firm's information securely, implementing indemnification provisions in the event of a cyberattack or requiring the third party to use specific safeguards.

As observed by many constituencies during the notice and comment process for the pending rulemaking, there are compelling arguments against adoption the SEC's proposal. Among other concerns, disclosure of a cyber incident may interfere with ongoing law enforcement investigations into an intrusion. And publicly identifying vulnerabilities and changes in cybersecurity policies may also encourage repeat attacks. Companies will have to account for these potentially competing considerations when deciding what to disclose, how much to disclose, and when to do so.

Regulated Entities. As with public companies, regulated entities should assess the adequacy of their existing cybersecurity protections and update them in light of the SEC's new proposals and enforcement actions. Such an assessment should include a review of (1) the nature, sensitivity and location of information that the entity collects, processes and/or stores; (2) internal and external cybersecurity threats to and vulnerabilities of the entity's information and technology systems; (3) security controls and processes currently in place; (4) the likely impact if the information or technology systems become compromised; (5) the effectiveness of the governance structures for the management of cyber risks; (6) the procedures in place for detecting, responding to and escalating awareness of cyber incidents; and (7) the policies and procedures in

place for providing training and guidance to the firm's personnel to ensure that best practices are followed.

Proactive compliance is key. Prior to the rules' adoption, regulated entities should establish comprehensive cybersecurity risk management programs; have in place risk-based policies and procedures that non-lawyers can understand, and update those policies in response to evolving threats; provide mandatory training to employees on cyber threats, policies and procedures; invest resources in security; and anticipate cyber-focused examinations.

The SEC's cyber-regulatory overhaul is fast approaching. In light of these impending changes, companies, advisers and other regulated entities should proactively review their cybersecurity policies, procedures and controls, and make enhancements to their cyber compliance function with the SEC's proposed rules in mind.

Brian Finch, a Pillsbury Public Policy partner with extensive regulatory and government affairs advocacy experience, is a recognized authority on global security and cybersecurity threats. Brian in particular focuses his practice on assisting clients with matters involving cyber security, national defense and intelligence policies, homeland security concerns, and in general providing proactive advice to mitigate liability in the event of a significant security incident.

David Oliwenstein, formerly with the SEC's Division of Enforcement, advises clients on complex investigations, regulatory and criminal enforcement of the securities laws, and securities litigation. Both in private practice and during his tenure at the SEC, David has handled matters involving insider trading, cybersecurity, digital assets, accounting misconduct, market manipulation, algorithmic trading, disclosure issues, ESG, and offering frauds.

			
You may also be interested in this PLI Program: SEC as Cyber Cop	**You may also be interested in this PLI Publication:** Cybersecurity Obligations for Attorneys: Confidential Information in the Age of Cyber Crime	**To submit an article for consideration, please contact the editor at** editor.plichronicle@pli.edu **or visit** pli.edu/PLIChronicle/contribute **for more information**	**Sign up for a free trial of PLI PLUS at** pli.edu/pliplustrial

Disclaimer: The viewpoints expressed by the authors are their own and do not necessarily reflect the opinions, viewpoints and official policies of Practising Law Institute.

This article is published on PLI PLUS, the online research database of PLI. The entirety of the PLI Press print collection is available on PLI PLUS—including PLI's authoritative treatises, answer books, course handbooks and transcripts from our original and highly acclaimed CLE programs.