CLCT

WILLIAM & MARY LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 16 | March 7, 2022

Table of Contents

Daniel Shin, research scientist with the Commonwealth Cyber Initiative (CCI) Coastal Virginia region, wants to hear from you! Submit any cybersecurity and information security news items or request related topics, via e-mail to dshin01@wm.edu.

This newsletter supports the mission of CCI. To learn more about CCI, including upcoming events, funded research, and news, please visit cyberinitiative.org.

The SEC proposes regulations on Cybersecurity Risk Management for Investment Advisers and Companies

On February 9, 2022, the Securities and Exchange Commission (SEC) voted by three to one to propose new regulations related to cybersecurity risk management for registered investment advisers, investment companies, and business development companies. *SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds*, available here; *Final Commission Votes for Agency Proceedings (February 2022)*, available here. Under the proposed regulation advisors and funds must:

1. Develop and implement cybersecurity policies and procedures aimed at addressing cybersecurity risks that could negatively impact advisory clients and fund investors;
2. Disclose publicly cybersecurity risks and "significant cybersecurity incidents" that occurred in the last two fiscal years; and
3. Follow new recordkeeping requirements that are designed to improve the transparency of cybersecurity-related information while facilitating the Commission's inspection and enforcement capabilities.

The SEC noted increasing cyber attacks targeting registered advisers and funds, and it determined that such incidents could cause substantial harm to clients and investors. *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, Release No. 33-11028 at 6-7, available here. On January 24, 2022, SEC Chair Gary Gensler commented that threat actors target various entities and businesses "[t]o steal data, intellectual property, or money; lower confidence in [the U.S.] financial system; disrupt economies; or just demonstrate [the threat actor's] capabilities." *Cybersecurity and Securities Laws*, available here. The Commission's focus on cybersecurity risk management and transparency practices attempts to protect investors' interests within the evolving threat landscape while further facilitating orderly and stable conditions for the U.S. capital markets. *See What We Do [U.S. Securities and Exchange Commission]*, available here.

The proposed regulation is subject to a public comment period, which is expected to conclude by April 11, 2022.

Current SEC Cybersecurity Guidelines and Regulations

Cybersecurity Incident Disclosure Requirements

Covered entities, including listed companies, have a legal obligation to meet reporting requirements intended to inform investors and the Commission of relevant facts about the state of the entity. *See The Laws That Govern the Securities Industry [Investor.gov]*, available here.

On October 13, 2011, SEC's Division of Corporation Finance published its guidance on disclosure requirements with respect to cybersecurity and cyber incidents. *CF Disclosure Guidance: Topic No. 2*, available here. Although federal securities laws do not explicitly mention cybersecurity or cyber incidents, the Division's cybersecurity disclosure guidance concluded that existing disclosure rules require covered entities to disclose cybersecurity incidents publicly to investors and the SEC. *Id.* ("[A] number of disclosure requirements may

impose an obligation on registrants to disclose such risks and incidents. In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures.").

On February 20, 2018, SEC Commissioners approved and published the agency's interpretative guidance on disclosure requirements concerning cybersecurity risks and incidents, which strengthened and expanded the Division of Corporation Finance's prior guidance. *Statement on Cybersecurity Interpretive Guidance*, available here. (The 2018 interpretative guidance also addressed the topics of implementation of cybersecurity policies and procedures as well as the application of insider trading prohibitions in the cybersecurity context. *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Release No. 33-10459, available here.)

Complying with SEC's cybersecurity disclosure guidance, listed companies have promptly disclosed cybersecurity incidents. For example, on August 17, 2020, Carnival Corporation promptly reported a ransomware attack that occurred two days prior through its Form 8-K filing with the Commission. *Issue 3: CLCT Cybersecurity and Information Security Newsletter - Carnival reported ransomware attack and data breach in SEC filing*, available here.

Customer Information Safeguard Requirements

Rule 30(a) of Regulation S-P, commonly referred to as the "Safeguard Rule," sets out the requirements for every broker, dealer, investment company, and registered investment adviser to safeguard customer records and information. 17 C.F.R. 248.30, available here. The Safeguard Rule requires covered entities to implement policies and procedures aimed at protecting customer records and information using administrative, technical, and physical means. *Id.* Specifically, these policies and procedures must reasonably be designed to:

1. Maintain the security and confidentiality of customer records and information;
2. Protect against any anticipated threats or disruptions to the security or integrity of customer records and information; and
3. Protect against unauthorized access to or use of customer records or information that could result in substantial harm or *inconvenience* to any customer.

The Safeguard Rule also sets out certain data disposal requirements involving consumer report information and records. *See 17 C.F.R. 248.30(b)*, available here.

On August 30, 2021, the SEC sanctioned eight firms for their failure to adhere to the Safeguard Rule during a series of cyber incidents involving unauthorized email account takeovers. *SEC Announces Three Actions Charging Deficient Cybersecurity Procedures*, available here. At the time, the Commission alleged that sanctioned firms failed to either adopt required policies and procedures consistent with the Safeguard Rule, or to implement fully those policies and procedures across their firms' IT systems.

Analysis

The proposed SEC rules aim to bolster the Safeguard Rule requirements while implementing additional transparency to the cybersecurity risk landscape among covered entities. The Commission notes that the three major components of the proposed regulation, taken together, provide a comprehensive framework to address cybersecurity risks for advisers and funds, and give clients and investors better information to facilitate investment decisions.

Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, *supra* at 14-15.

Although the proposed rule provides a much-needed baseline for strengthening financial and investment sector cybersecurity, it fails to clarify what constitutes adequate and reasonable cybersecurity policies and procedures. The Commission recognized that "there is not a one-size-fits-all approach to addressing cybersecurity risks," especially "given the number and varying characteristics (*e.g.,* size, business, and sophistication) of advisers and funds" in the industry. *Id.* at 15, 17. The proposed regulation would allow each firm to tailor its cybersecurity program to the nature and scope of its business.

The proposed regulation provides a set of minimum required components for proper cybersecurity policies and procedures. The Commission is clear that the responsibility of determining key details is the individual firm's responsibility. However, the issue with the proposed regulation is the lack of a set of illustrative or minimum cybersecurity policies and procedures that covered entities could rely on when designing their own programs.

The SEC does provide references to resources furnished by other federal agencies to help covered entities develop their cybersecurity policies and procedures. *Id.* at 17 n.24 ("Funds and advisers may wish to consult a number of resources in connection with these elements. *See, e.g.,* National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Apr. 16, 2018) . . . ; Cybersecurity and Infrastructure Security Agency (CISA), *Cyber Essentials Starter Kit – The Basics for Building a Culture of Cyber Readiness* (Spring 2021) . . . . "). However, those referenced resources alone do not provide clear guidance on whether a particular cybersecurity policy and procedure is *reasonable* for a particular firm from a regulatory compliance perspective. The ambiguity of what constitutes "reasonable" cybersecurity policies and procedures makes it difficult for covered entities to determine whether their cybersecurity risk management processes comply with the proposed regulation. At a minimum, the Commission should consider releasing sample "blueprints" of cybersecurity policies and procedures for categories of firms to consult during their cybersecurity policy and procedure drafting process.

As noted above, the proposed cyber risk management regulation did not receive unanimous support among SEC Commissioners. Opposing the proposed regulation, SEC Commissioner Hester M. Peirce wrote in her dissent that "[t]he Commission, serving as a repository with up-to-date intelligence on trends in financial sector cybercrime, could provide registrants with practical, timely knowledge so vital to keeping one step ahead of the bad guys." *Statement on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, available here. Commissioner Peirce criticized the proposed rule as potentially becoming "an easy hook for an enforcement action, even when a firm has made reasonable *efforts* to comply with the prescriptions." *Id.* (emphasis added).

Although the Commission's proposal for mandatory cybersecurity incident disclosures and recordkeeping requirements provides much-needed visibility in the cybersecurity threat landscape within the financial and investment sector, the cybersecurity policy and procedure requirements, without further clarification, may provide more regulatory confusion than resilient cybersecurity implementation among covered entities.

FBI, NSA, and CISA issue Joint Cybersecurity Advisory alert with respect to State-sponsored Cyber Attacks on Cleared Defense Contractor Networks

On February 16, 2022, the Cybersecurity and Infrastructure Security Agency (CISA) published a joint cybersecurity advisory (Joint Advisory) that warned U.S. cleared defense contractors (CDCs) about being targeted by Russian state-sponsored state actors (State Threat Actors). *Alert (AA22-047A)*, available here. The Joint Advisory stated that the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and CISA observed State Threat Actors targeting CDCs from as early as January 2020 through the present.

According to the Joint Advisory, State Threat Actors used:

1. Bruteforcing techniques to access potentially compromised enterprise and cloud-based accounts, especially Microsoft Office 365 accounts;
2. Spearphishing emails to solicit victims to downloading malicious programs to CDC's computers; and
3. Exploiting software vulnerabilities to gain unauthorized access to higher privileges on CDCs' IT systems.

Although State Threat Actors were observed using conventional cybersecurity intrusion techniques to access CDC's systems, the Joint Advisory noted that they have "acquired unclassified CDC-proprietary and export-controlled information." The report does not explicitly mention whether classified information was obtained by State Threat Actors, but it does mention that sensitive data about U.S. defense and intelligence programs and capabilities may have been accessed.

CDCs supporting the U.S. Army, U.S. Air Force, U.S. Navy, U.S. Space Force, and Department of Defense and Intelligence programs have been affected by State Threat Actors' cyber operations. To remedy the situation, the Joint Advisory provides a list of cybersecurity best practices to manage, detect, and respond to cyber threats posed by threat actors.

Analysis

During the Kaseya attack, where threat actors used a supply chain attack to distribute ransomware to thousands of businesses, one major difficulty that stymied security researchers initially was the malicious code that continuously erased system logs to delete traces of its activity. *Crticial [sic] Ransomware Incident in Progress*, available here. Due to a community-wide effort, security researchers were able to gather server logs to piece together forensic clues on the malicious code.

Among various technical recommendations, the Joint Advisory advises CDCs to implement robust log collection and retention practices to facilitate the detection of malicious applications and network activity. Without secure and proper log management, targeted CDCs would have their cyber incident detection and investigation capabilities severely hampered.

One of the shortcomings of the Joint Advisory is its lack of emphasis on reporting cyber incidents to a centralized federal government entity. Although the Joint Advisory provides contact information of the FBI, NSA, and CISA, it fails to *urge* potential victim CDCs to report cyber incidents to the federal government. Given that State Threat Actors are likely conducting cyber attacks across various CDCs' IT networks in a systematic pattern for intelligence gathering, having macro visibility of the CDCs' cyber threat landscape is critical for federal agencies to potentially coordinate defensive countermeasures.

The need for centralized federal cyber incident reporting has been recognized by the U.S. Senate. For example, the *Cyber Incident Notification Act of 2021*, a bill introduced by Senator Mark Warner, would mandate cyber breach notifications by federal agencies, *federal contractors*, and critical infrastructure operators to CISA. *Issue 10: CLCT Cybersecurity and Information Security Newsletter - Senator Warner introduced legislation to bolster cyber breach notification*, available here. As of the publication of this newsletter, the bill has been referred to the U.S. Senate Committee on Homeland Security and Governmental Affairs. Similarly, the *Strengthening American Cybersecurity Act of 2022*, a bill introduced by Senator Gary Peters that passed in the U.S. Senate, provides a comprehensive set of laws aimed at strengthening the cybersecurity landscape in the U.S. *S.3600 - Strengthening American Cybersecurity Act of 2022*, available here. The legislation sets out new cybersecurity reporting requirements (e.g., cyber incident disclosures) for critical infrastructure entities. (The next issue of the newsletter will provide a detailed analysis of this important legislation.)

Even though there is no federal statutory requirement for CDCs to report promptly any significant cyber incidents to a centralized federal agency, the Joint Advisory could have taken the opportunity to encourage strongly CDCs to report cyber incidents to a federal agency. During the 2021 Kaseya attacks, the reason why the private-sector cybersecurity community was able quickly to identify and examine the complex malicious code was due to victims of the attack sharing digital evidence (e.g., logs of the attack) to security experts. It is anticipated that if the federal government can encourage its private contractors to be more collaborative in their efforts of sharing information with respect to cybersecurity incidents, CISA and its federal agency partners could offer more effective and coordinated assistance to resolve cyber issues industry-wide.