X. Public Corporations and Cybersecurity

A. Introduction

Since the internet boom in the early 2000's, cybersecurity risks have developed into significant threats to investors, markets, and the economy in general.[1][ES: Changes as made. No plagiarism.] "Whether it is the companies in which investors invest, their accounts with financial services firms, the markets through which they trade, or the infrastructure they count on daily, the investing public and the U.S. economy depend on the security and reliability of information and communications technology, systems, and networks."[2] Corporations have largely moved operations and the storage of confidential information to digital platforms and the opportunity to exploit that transition have led to serious risks to the markets and economies of the world.[3]

"Cybersecurity incidents can result from unintentional events or deliberate attacks by insiders or third parties, including cybercriminals, competitors, nation-states, and 'hacktivists.'"[4] According to The U.S. Securities and Exchange Commission ("SEC"), negative effects created by cybersecurity breaches include: remediation costs, such as liability for stolen assets or information; increased cybersecurity protection costs, which may include the costs of making organizational changes; reputational damage that adversely affects customer or investor confidence; litigation and legal risks; and most importantly, damage to the company's competitiveness, stock price, and long-term shareholder value.[5]

This article explores the possible changes to regulations regarding cybersecurity and their effects on the public sector. Section 2 reviews the recent cybersecurity trends that led to increased focus on the topic by the SEC and analyzes prior guidance from the SEC regarding cybersecurity. Section 3 reviews recent actions taken by other government branches to resolve this issue, and the new regulations' relevance to the current financial landscape. Section 4 analyzes recent

---

[1] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 C.F.R. §§ 229, 249 (Sec. Exch. Comm'n, Feb. 26, 2018).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*

SEC settlements with companies regarding cybersecurity issues and how these actions may shed light on the upcoming SEC guidance.

B. History

In the past decade, the SEC has continuously monitored these "new age" threats of security related to technology, proposing rules for corporations to follow to avoid potential attacks and limit the consequences of these attacks.[6] The goal of the SEC in implementing these new rules is to create transparency for investors and other interested parties by eliminating elective disclosures and deterring corporations from refraining from disclosing material information.[7]

In October 2011, the SEC's Division of Corporation Finance (the "Division") issued guidance that provided the Division's views regarding disclosure obligations relating to cybersecurity risks and incidents.[8] The guidance explains that, "[a]lthough no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents," companies nonetheless may be obligated to disclose such risks and incidents.[9] After the issuance of the guidance, many companies included additional cybersecurity disclosure, typically in the form of risk factors, which marked a large first step as cybersecurity guidance developed throughout the 2010s.[10]

In 2018, the SEC offered two additional recommendations to address developments in the cyber space following 2011.[11] First, the guidance stressed the "importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents."[12] This was in response to companies not properly diagnosing attacks and

---

[6] Vivek Mohan, *David Simon & Richard Rosenfeld, SEC Increasingly Turns Focus Toward Strength of Cyber Risk Disclosures,* HARV. L.F. ON CORP. GOVERNANCE (July 25, 2021). *https://corpgov.law.harvard.edu/2021/07/25/sec-increasingly-turns-focus-toward-strength-of-cyber-risk-disclosures/ [https://perma.cc/4YBA-JGNF].*

[7] *Our goals*, U.S. SEC. EXCH. COMM'N, https://www.sec.gov/our-goals (Oct. 16, 2018)) [https://perma.cc/ZH9C-MTGL].

[8] CF Disclosure Guidance: Topic No. 2—Cybersecurity, U.S. SEC. EXCH. COMM'N (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [https://perma.cc/KWX5-5BQH].

[9] *Id.*

[10] *Id.*

[11] 17 C.F.R. §§ 229, 249, *supra* note 1, at 6.

[12] *Id.*at 6.

reposing them to the SEC or to investors.[13] Additionally, the update reminded companies and their "directors, officers, and other corporate insiders of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws."[14] In particular, the SEC pointed to the "obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents."[15] This rule protects investors and further promotes investment by ensuring detrimental material facts are disclosed before investment.[16]

C. Actions by Other Government Branches

By the end of 2021, the SEC was expected to propose new rules that will again reshape the guidance in regards to protecting corporations and their investors from cyber threats, though this guidance was pushed back to 2022 due to other regulatory issues.[17] Although there is not much available information about the new rules yet, we can speculate on certain policy points based on recent actions by the government. First, these rules will likely draw some inspiration from the Internet of Things Cybersecurity Improvement Act of 2020 that was enacted by Congress.[18] While the Act applies to government agencies, the goal was to establish "standards and guidelines for the Federal Government on the appropriate use and management by agencies of Internet of Things devices owned or controlled by an agency and connected to information systems owned or controlled by an agency."[19] These standards hold similarities to the SEC proposals in 2011 and 2018, in that they provide strict guidelines for how companies develop their internal cybersecurity policies and react to attacks, and these standards will likely be a focal

---

[13] Mohan, Simon & Rosenfeld, *supra* note 6.
[14] 17 C.F.R. §§ 229, 249, *supra* note 1, at 7.
[15] *Id.*at 7.
[16] *Id.*
[17] *Press Release, SEC, SEC Announces Annual Regulatory Agenda (June 11, 2021) (on file with author)*
[18] *Rajesh De Et Al., President Biden Issues Executive Order to Improve Nation's Cybersecurity,* MAYER BROWN, (May 17, 2021), https://www.mayerbrown.com/en/perspectives-events/publications/2021/05/president-biden-issues-executive-order-to-improve-nations-cybersecurity [https://perma.cc/ZJ27-9MMT]
[19] Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, 134 Stat. 1001. [ES: This is where the quote is from → https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.htm].

point of the 2021 rules.[20] This Act also follows a legislative trend created by Congress in 2015 with The Cybersecurity Information Sharing Act of 2015.[21] There, Congress authorized "companies to monitor and implement defensive measures on their own information systems to counter cyber threats," creating more room for companies to handle cybersecurity attacks without unnecessary fear of legal repercussions.[22] Further, the Act established certain protections to "encourage companies voluntarily to share information—specifically, information about 'cyber threat indicators' and 'defensive measures'—with the federal government, state and local governments, and other companies and private entities."[23] These provisions allow the companies to act on and report cybersecurity attacks with protection from liability, non-waiver of privilege, and protections from FOIA disclosure, ensuring that attacks are fully documented and dealt with in a timely fashion.[24] These legislative acts likely shine a light on the rules and guidelines that the SEC plans to release in October.

The new rules follow President's Biden's Executive Order on Improving the Nation's Cybersecurity (Cyber EO) from May of 2021, which offered additional insight into the expected updates from the policies instilled in 2018.[25] "The Cyber EO addresses four general topics across eight operative sections" in both private and public sectors: "(a) increasing information sharing from the private sector to the federal government[]; (b) enhancing the security of software purchased by federal agencies[]; (c) establishing a Cyber Safety Review Board[]; and (d) improving the cybersecurity posture of the federal government."[26] For the most part, the Cyber EO did not address the security of consumer products.[27] It did, however, establish security labeling programs of the Internet of Things, intending to inform both the government and the

---

[20] *Id.*

[21] *Brad S. Karp, Paul, Weiss, & Rifkind, Federal Guidance on the Cybersecurity Information Sharing Act of 2015, HARV. L.F. ON CORP. GOVERNANCE (March 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ [https://perma.cc/C9KQ-M2JS]*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] Rajesh De et al., *supra* note 18.

[26] *Id.*

[27] *Id.*

public on whether software was developed in compliance with security requirements. [28]

These rules have clear relevance in the current financial landscape as corporations, financial institutions, and investors transfer their businesses and interactions to an almost completely digital footprint.[29] The importance of these rules draw from the need for equal access to material facts by all investors to avoid insider trading based on cyber-attacks, as insiders within companies hit with cybersecurity attacks may have the ability to trade on the information before it is available to the public.[30] Along those lines of transparency, the SEC has shown in their statements and proposed rules of the past that they will offer leniency and liability protection for companies that report attacks, hoping to encourage firms to operate and detect attacks without fear of negative repercussions.[31] In a more macro sense, the overall goal for the SEC is to promote the economy and make investors and customers feel more secure that their information will not be stolen and used to extort them, leading to more market activity across the board.[32]

D. SEC Cybersecurity Disclosure Settlements

Beyond direct guidance offered by the SEC, early enforcement trends from SEC Chairman Gary Gensler provide a picture of how his administration will act towards cybersecurity concerns and build on the prior administration's initiatives.[33] From 2017 to 2020, the prior administration, under Chairman Jay Clayton, focused efforts largely on protecting retail investors from cyberattacks.[34] During Clayton's tenure, the SEC created a cyber unit responsible for protecting retail investors from cyber threats.[35] This unit led investigations into large companies

---

[28] *Id.*
[29] 17 C.F.R. §§ 229, 249, *supra* note 1.
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] Julianne Landsvik, Randall Lee & Michael Welsh, *Early SEC Enforcement Trends from chairman Gensler's first 100 Days*, THE HARV. L. SCH. F. ON CORP. GOVERNANCE (Aug. 11, 2021), https://corpgov.law.harvard.edu/2021/08/11/early-sec-enforcement-trends-from-chairman-genslers-first-100-days/ [https://perma.cc/TG2L-YYV7]
[34] *Id.*
[35] Press Release, SEC, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors, (Sept. 25, 2017) (on file with author)

for disclosure deficiencies, including the successful investigation of Yahoo! for "allegedly misleading investors by failing to disclose a large data breach."[36] However, the administration under Clayton did not put an emphasis on pursuing disclosure violations beyond instances of direct breaches by third parties due to insufficient protocol within a company.[37]

In contrast, Gensler has already shifted the SEC's focus further towards disclosure violations since he was sworn into the Chairman position in April 2021.[38] In June, just two months after being sworn in, Gensler's division "announced settled charges against title insurer First American Financial Corporation arising out of the company's disclosures regarding past cybersecurity incidents."[39] The SEC charged First American with a violation of Rule 13a-15(a), which requires companies to maintain internal control and rules surrounding disclosure and ensure management is aware of any potentials for breach.[40] The SEC noted that "[a]s a result of First American's deficient disclosure controls, senior management was completely unaware of this vulnerability and the company's failure to remediate it."[41] The chief of the SEC Cyber Unit, Kristina Littman, stated in the SEC's announcement of the settlement in June 2021 that "issuers must ensure that information important to investors is reported up the corporate ladder to those responsible for disclosures."[42] This case was significant as it was "one of the first instances in which the SEC had brought charges in the absence of an actual data breach or intrusion by a third party."[43] This marked a dramatic shift from the policies under Clayton, as the violation was found based strictly on internal policies, rather than as a response to an attack.[44]

---

[36] Landsvik, Lee & Welsh, *supra* note 33.
[37] *Id.*
[38] *Id.*
[39] Press Release, SEC, SEC Charges Issuer with Cybersecurity Disclosure Controls Failures (June 15, 2021) (on file with author)
[40] Final rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, 17 C.F.R. § 210-74 (2003),
[41] SEC, *supra* note 39.
[42] Landsvik, Lee & Welsh, *supra* note 33.
[43] *Id*.
[44] *Id.*

In August, the SEC took additional action against public companies that did not give adequate disclosure of cyberattacks.[45] The three settlements released in August targeted eight investment advisor and broker-dealer firms, with each firm experiencing "compromises of [their] email accounts (many of which were maintained on cloud-based systems) that arose from alleged failures or lapses in their cybersecurity policies and procedures."[46] These lapses in policies led to personally identifying information from thousands of customers and clients of these firms being exposed to hackers and otherwise put these consumers at risk.[47] In particular, the settlement involving Cetera indicated that the Enforcement Division may be open to pursuing "more novel enforcement theories" based on a firm's response to a cybersecurity matter, accounting for the evolution of cybersecurity attacks and risks in recent years.[48] Following these settlements, the SEC made clear that "firms must ensure that they are enforcing existing cyber policies and procedures across the entire firm (including consultants and temporary employees who may have access to—or whose credentials may be used to access—confidential customer information such as PII)."[49] This furthered the comments made by the SEC in their statement about the settlement with Cetera, where the company had violated their own policies in failing to modify disclosures to customers' whose personal information had been leaked due to a cybersecurity breach.[50]

In addition to these actions against companies directly, the SEC has emphasized increased disclosures without targeting specific attacks. Following the cyberattack on SolarWinds, the SEC requested that hundreds of companies voluntarily provide information about recent attacks, offering limited immunity from enforcement action in return for compliance.[51] SolarWinds was the target of a cyberattack that had a ripple effect for hundreds of public companies, which had their customers' information leaked as a result of the attack.[52] These affected

---

[45] Allison Bernbach, William LaBas & Michael Osnato, *Key takeaways from recent SEC cybersecurity charges*, THE HARV. L. SCH F. ON CORP. GOVERNANCE (Oct. 1, 2021), https://corpgov.law.harvard.edu/2021/10/01/key-takeaways-from-recent-sec-cybersecurity-charges/ [https://perma.cc/6ZUD-QRAP]
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] Landsvik, Lee & Welsh, *supra* note 33.
[52] *Id.*

companies were required to disclose all cyberattacks since October 2019 to receive the partial immunity, allowing more transparency for the SEC and retail investors alike regarding these public companies.[53] This decision from the SEC was significant, as the requests came from the acting director of the Division of Enforcement, which was highly unusual as requests usually came from lower ranking officials.[54] Additionally, the wide scope of the request, spreading across hundreds of companies, displayed the expansion of the SEC's efforts beyond isolated incidents and led to the companies reevaluating and enhancing their internal policies regarding cybersecurity, regardless of whether they had any attacks to report.[55]

These enforcement actions and requests made by the SEC in just the last six months add additional insight into how expansive the upcoming guidance will be in regards to cybersecurity disclosures. Gensler has made it clear that cybersecurity will be a priority for the SEC, and strict enforcement of disclosure rules will become routine as technology continues to develop.[56] Companies will likely have to rethink, and possibly overhaul, their internal procedures regarding potential attacks to ensure that they do not face substantial enforcement action due to inaction or delayed reporting of cybersecurity issues they deal with. While the 2011 and 2018 rules create a framework for what is expected of public companies, the new regime leading the SEC likely intends to dramatically increase the scrutiny given to public companies and eliminate any grey areas regarding disclosure of nonpublic cyberattack information that should be available to retail investors.

[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*

E. Conclusion

As blockchains, cryptocurrencies, and other advances in business and technology move the operations of corporations to digital mediums, cyberattacks become a greater threat to investors and the corporations they invest in. While the atmosphere of cybersecurity within the financial sector is continuously changing, the upcoming SEC proposal should provide increased insight into the path that the government is taking to educate corporations and investors to prevent the threat.

Joshua Stein[57]

[57] Student, Boston University School of Law (J.D. 2023).