COMMENTS

THE ROAD TO THE RULES: THE SEC MANDATES CYBERSECURITY DISCLOSURES*

I. INTRODUCTION

Locky, Phoenix, WannaCry, DarkSide, NotPetya, Hades. Do these names sound familiar? They have each touched the lives of individuals across the globe, generated revenues in the seven to eight figures, and managed to stand out in a field crowded with other actors. No, these are not the names of Disney antiheroes. They are not TikTok superstars. They are the names of just a few of the large-scale cyberattacks of the past ten years.[1] The World Economic Forum (WEF) paints a stark picture of cybersecurity risk today: "[G]rowing cyberthreats are outpacing societies' ability to effectively prevent and manage them."[2] Patchwork government oversight and a global shortage of cybersecurity professionals have only aided this acceleration in cybercrime.[3] Additionally, cybercriminals face little risk of extradition or prosecution, due to the absence of a cooperative international response and the unwillingness of some nations to address cybercrime originating within their borders.[4]

---

* Lisa López, J.D. Candidate, Temple University Beasley School of Law, 2024. The author formerly worked in K-12 education, in administration, technology, and teaching roles. Thank you to Professor Duncan Hollis for his guidance and input. Tremendous thanks to the entire *Temple Law Review* staff for their thoughtful editing, with special appreciation to the always precise and perseverant Mara Poulsen and Jay Kaplan. Most importantly, thank you to my family for all of your patience and grace.

1. *See* Amy Deen Westbrook, *A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets, and Defending National Security*, 18 N.Y.U. J.L. & BUS. 391, 402, 409, 430 (2022); Lawrence J. Trautman & Peter C. Ormerod, *Wannacry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 505–06 (2019) [hereinafter Trautman & Ormerod, *Emerging Threat*].

2. WORLD ECON. F., THE GLOBAL RISKS REPORT 2022, at 47 (17th ed. 2022) [hereinafter GLOBAL RISKS REPORT 2022].

3. *Id.*

4. *See id.* at 49; *see also* Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1026 (2018) ("A focus on national security will require closer cooperation between the United States and other nations . . . ."). There is recent evidence, though, that certain countries are more willing to cooperate to address the explosive growth of cyberthreats. *See* Memorandum from Anne Neuberger, Deputy Assistant to the President and Deputy Nat'l Sec. Advisor for Cyber and Emerging Tech., to Corporate Executives and Business Leaders (June 2, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf [https://perma.cc/2JXE-U69V] ("[T]he Federal Government is . . . working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.").

Losses from cyberattacks in the United States can be felt at the national economy level,[5] and attacks on individuals have been replaced with targeted, large-scale assaults on specific companies.[6] When a publicly traded corporation is attacked, the damage extends beyond the organization and inflicts financial losses on shareholders.[7] A 2021 study found that, on average, a successful cyberattack decreased shareholder wealth by $495 million in the three-day window after the event.[8] The highly publicized 2017 cyberattack on the credit reporting giant Equifax, for example, erased $6 billion in market capitalization.[9]

U.S. laws that address cybersecurity lack coordination and do not fully respond to the realities of corporate cybersecurity risk.[10] One commentator described the patchwork of statutes and regulations that do address cybersecurity as an "uncoordinated mishmash" of laws, not designed to operate in conjunction with one another.[11] Additionally, gaps in the scope of cybersecurity laws leave corporate cybersecurity largely unaddressed—state laws have focused on protecting the personal data of individuals,[12] while the federal government has primarily directed its initiatives

5. Though attempts to accurately measure the impact of cyberattacks are notoriously difficult, a recent rigorous effort to pinpoint cyberattack costs estimated the upper bound of 2016 losses in the U.S. economy at $770 billion, or 4.1% of total GDP. DOUGLAS THOMAS, U.S. DEP'T OF COM., CYBERCRIME LOSSES: AN EXAMINATION OF U.S. MANUFACTURING AND THE TOTAL ECONOMY 20 (2020) (using public data from the Bureau of Justice Statistics, together with uncertainty analysis methods). *See also* OFF. OF COMPLIANCE INSPECTIONS & EXAMINATIONS, SEC, CYBERSECURITY AND RESILIENCY OBSERVATIONS 1 (2020) [hereinafter CYBERSECURITY AND RESILIENCY OBSERVATIONS] https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf [https://perma.cc/W8FW-XQGY] ("The seriousness of the threats and the potential consequences to investors, issuers, and other securities market participants, and the financial markets and economy more generally, are significant and increasing.").

6. Ronny Richardson, Max M. North & David Garofalo, *Ransomware: The Landscape Is Shifting—A Concise Report*, 17 INT'L MGMT. REV. 5, 5–6 (2021).

7. *See* CYBERSECURITY AND RESILIENCY OBSERVATIONS, *supra* note 5, at 1.

8. Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis & René M. Stulz, *Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms*, 139 J. FIN. ECON. 719, 721 (2021) (representing a 0.84% average shareholder value loss; value loss averaged 1.09% if the attack included loss of personal financial information). The study looked at disclosed cyberattacks on public corporations from 2005 to 2017. *Id.* at 720, 727.

9. AnnaMaria Andriotis, Michael Rapoport & Robert McMillan, *'We've Been Breached': Inside the Equifax Hack,* WALL ST. J. (Sept. 18, 2017, 8:04 AM EST), https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318 [https://perma.cc/8WBR-YC4F].

10. Kosseff, *supra* note 4, at 988.

11. *Id.*; *see, e.g.*, *id.* at 1000–01 (noting the example of healthcare, where "[i]t is inevitable that highly sensitive information and systems . . . may face more rigorous laws than in other areas, but those laws should not function in a black box"). Key federal cybersecurity regulations imposing sector-specific requirements are the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act, which addresses the financial sector. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 5–42 U.S.C.); Pub. L. No. 106-102, 113 Stat. 1338 (1999).

12. Kosseff, *supra* note 4, at 1010–11 ("[T]he existing cybersecurity framework focuses largely on . . . protecting individual privacy. However, the laws could be improved to focus more [on] other aspects, including: (1) integrity and availability, (2) protecting systems and networks; and (3) promoting economic and national security interests.").

at protecting critical infrastructure.[13] As a United Nations investigation asserts, relative to other countries, U.S. cybersecurity legislation is less centralized and "comparatively underdeveloped."[14]

Only recently, following a number of high-profile attacks on major American corporations, have federal agencies begun to consider the broader range of cybersecurity concerns affecting companies.[15] The Securities and Exchange Commission (SEC) is among U.S. regulators beginning to turn their attention to gaps in cybersecurity oversight. SEC Chair Gary Gensler has stated that "[c]ybersecurity is a team sport,"[16] and the SEC sees itself as a key player on that team. The SEC grounds its authority for cybersecurity oversight in its mission to protect investors and ensure the integrity of financial markets. Chair Gensler asserted, in 2022, that "[c]yber relates to each part of [the SEC's] three-part mission: investor protection, facilitating capital formation, and that which is in the middle, promoting fair, orderly, and efficient markets."[17]

Finalized in July 2023, and over a decade in the making, the SEC's Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure ("Cybersecurity Rules")[18] apply the long-established SEC corporate disclosure framework to the cybersecurity events, risks, and strategies of publicly traded companies. The Rules present both opportunities and challenges. Uniform, mandatory disclosures have the potential to spotlight successful cybersecurity practices as industry models and to lay plain the gaps and deficiencies that make some companies more vulnerable to a cyberattack. Risk assessment firm Moody's suggested that the Rules would "provide more transparency into an otherwise opaque but growing risk, as well as more consistency and predictability," and that "[i]ncreased disclosure should help

13. *See* Press Release, White House, Ongoing Public U.S. Efforts to Counter Ransomware, (Oct. 13, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/ [https://perma.cc/7U3P-YK7R] (detailing Biden administration initiatives to address cyberthreats); Neuberger, *supra* note 4; Jennifer Steinhauer, *House Passes Cybersecurity Bill After Companies Fall Victim to Data Breaches,* N.Y. TIMES (Apr. 22, 2015), https://www.nytimes.com/2015/04/23/us/politics/computer-attacks-spur-congress-to-act-on-cybersecurity-bill-years-in-making.html [https://perma.cc/MNT2-TDWE].

14. PRINCIPLES FOR RESPONSIBLE INV., U.N., STEPPING UP GOVERNANCE ON CYBER SECURITY 5 (2018), https://www.unpri.org/download?ac=5134 [https://perma.cc/Y359-SXM7].

15. *See* Press Release, White House, *supra* note 13; Steinhauer, *supra* note 13.

16. Gary Gensler, Chair, SEC, "Working On 'Team Cyber,'" Remarks Before the Joint Meeting of the Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Sector Coordinating Council (FSSCC), (Apr. 14, 2022) (quoting Jen Easterly, Dir., CISA, Cybersecurity Summit 2021 Keynote Address (Oct. 6, 2021), https://www.cisa.gov/resources-tools/resources/cybersecurity-summit-2021-summit-keynote [https://perma.cc/G6F5-Y6GB]), https://www.sec.gov/news/speech/gensler-speech-joint-meeting-041422 [https://perma.cc/XL9P-3WH6].

17. *Id.*

18. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Securities Act Release No. 11,216, Exchange Act Release No. 97,989, 88 Fed. Reg. 51896 (Aug. 4, 2023) [hereinafter SEC 2023 Cybersecurity Rules]; Press Release, SEC, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, 2023-139 (July 26, 2023), https://www.sec.gov/news/press-release/2023-139 [https://perma.cc/ZV44-D2YD].

companies compare practices and may spur improvements in cyber defenses . . . ."[19] Nonetheless, the Rules provide little guidance on the application of the materiality standard to this emerging and shifting area of risk and oversight.[20] While the materiality standard has historically been plagued by a lack of clarity in its application to other areas of disclosure, it is particularly problematic in the context of cybersecurity.[21] Additionally, companies are understandably concerned about the inherent dangers of disclosing the details of an in-process cyberattack.[22]

This Comment examines the interplay of two forces in the dynamic cyberthreat environment in which U.S. companies operate: on one side, corporate boards face an imperative to preserve and grow shareholder value in the looming shadow of cyber-threats and, on the other side, the SEC aims to fulfill its mission to facilitate information-sharing with shareholders and securities markets. Part II.A of the Overview provides a snapshot of the current state of corporate cyber-risk. Part II.B details the harms that cyberattacks inflict on American corporations. Part II.C discusses the challenges of corporate cybersecurity planning. Part II.D examines the role of corporate boards in cybersecurity oversight and cybersecurity risk management. Finally, Part II.E examines the evolution of the SEC's cybersecurity disclosure requirements and its 2023 Cybersecurity Rules.

The Discussion evaluates the shortcomings of the SEC's past approach to cybersecurity and considers the potential of the new Rules to incentivize engaged and effective cybersecurity oversight by corporate boards. The Discussion also addresses two significant unresolved issues—the materiality standard that guides disclosure and the risks inherent in disclosing details of an in-process cyberattack.

II. OVERVIEW

A. Cyber-Threats Target American Corporations

Understanding cyberattack mechanisms and strategies is necessary to appreciate the challenges corporations face when addressing cybersecurity risk management. Cyberattacks are perpetrated with malicious programming code, also known as

19. Tim Starks with David DiMolfetta, *The SEC Has a Big, New Cyber Rule for Public Companies*, WASH. POST: THE CYBERSECURITY 202 (July 27, 2023, 6:48 AM EDT), https://www.washingtonpost.com/politics/2023/07/27/sec-has-big-new-cyber-rule-public-companies/ [https://perma.cc/F2XL-MQJ8] (statement of Lesley Ritter, Senior Vice President, Moody's Investors Service).

20. The SEC has specified that companies must determine if a cybersecurity incident is "material" by relying on the common law standard: "information is material if 'there is a substantial likelihood that a reasonable shareholder would consider it important' in making an investment decision, or if it would have 'significantly altered the "total mix" of information made available.'" See *infra* 191 and accompanying text discussing the SEC's proposed cybersecurity rules; *see also* TSC Indus. v. Northway, 426 U.S. 438, 449 & n.10 (1976); 17 C.F.R. § 229.105(a) (2023) (requiring a "discussion of material factors that make an investment . . . speculative or risky").

21. See *infra* notes 231–34 and accompanying text for a discussion of the unresolved issues related to the materiality standard.

22. See *infra* notes 237–40 and accompanying text for a discussion of concerns related to the requirement to disclose a cyberattack within four days of reaching a determination that it is material.

"malware."[23] In an estimated ninety-five percent of attacks, human error enables the initial entry of malware into a business's digital systems.[24] Humans open email attachments, visit virus-infected websites, and download files from instant messages during peer-to-peer connections.[25] Once inside, malware exploits existing vulnerabilities and often cripples multiple systems throughout a network.[26] Malware can cause a service slowdown or shutdown through a range of attack strategies, including distributed denial of service;[27] data espionage; theft, destruction, or manipulation of data; and ransomware.[28] Advances in quantum computing, artificial intelligence, and virtual reality compound the risks created by these strategies and enable new types of threats.[29]

This discussion of corporate cybersecurity risk focuses on ransomware, as it has been the cyberattack strategy of choice in many of the recent large-scale attacks on American companies,[30] and the rise in the use of ransomware marks a significant shift in the nature of financially motivated cybercrime.[31] The list of publicly traded

23. *2021 Top Malware Strains*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/uscert/ncas/alerts/aa22-216a [https://perma.cc/TMK8-CQ5B] (last updated Aug. 25, 2022) ("Malware, short for 'malicious software,' can compromise a system by performing an unauthorized function or process.").

24. Paul Mee & Rico Brandenburg, *After Reading, Writing and Arithmetic, the 4th 'R' of Literacy is Cyber-Risk*, WORLD ECON. F. (Dec. 17, 2020), https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education/ [https://perma.cc/B2G6-GGM2].

25. *Handling Destructive Malware*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY (Feb. 1, 2021), https://www.cisa.gov/news-events/news/handling-destructive-malware [https://perma.cc/S6CS-9NSW].

26. *Id.*; *see also* MULTI-STATE INFO. SHARING & ANALYSIS CTR., CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, RANSOMWARE GUIDE 2 (2020) [hereinafter RANSOMWARE GUIDE].

27. Kosseff, *supra* note 4, at 995 ("A [distributed denial of service] attack floods a targeted server with traffic from multiple sources, causing a slowdown in traffic or a complete shutdown."); *Understanding Denial-of-Service Attacks*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY (Feb. 1, 2021), https://www.cisa.gov/news-events/news/understanding-denial-service-attacks [https://perma.cc/MZY5-DTG2].

28. *See Understanding Denial-of-Service Attacks*, *supra* note 27; *Handling Destructive Malware*, *supra* note 25; RANSOMWARE GUIDE, *supra* note 26, at 2.

29. *Post-Quantum Cryptography*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/quantum [https://perma.cc/P6PT-2YVU] (last updated Oct. 4, 2022) ("[Quantum computing] is expected to break some encryption methods that are widely used to protect customer data, complete business transactions, and secure communications."); SEC 2023 Cybersecurity Rules, *supra* note 18, at 51898 ("[R]ecent developments in artificial intelligence may exacerbate cybersecurity threats, as researchers have shown that artificial intelligence systems can be leveraged to create code used in cyberattacks, including by actors not versed in programming."); GLOBAL RISKS REPORT 2022, *supra* note 2, at 47 (noting potential growth in the ability of nontechnical criminals to execute attacks using AI-powered malware); *id.* at 49 ("The emergence of the metaverse could also expand the attack surface for malicious actors by creating more entry points for malware and data breaches.").

30. *2021 Top Malware Strains, supra* note 23.

31. *See* JOSEPHINE WOLFF, YOU'LL SEE THIS MESSAGE WHEN IT IS TOO LATE: THE LEGAL AND ECONOMIC AFTERMATH OF CYBERSECURITY BREACHES 60 (2018).

American companies that faced ransom demands in 2021 and 2022 includes Apple,[32] Accenture,[33] Robinhood,[34] CNA Financial,[35] and Kronos.[36]

In early ransomware attacks, perpetrators used malware to encrypt a victim's files, effectively locking victims out of their own systems.[37] The victim was then presented with a demand for a ransom payment, in exchange for a decryption key.[38] By selling encrypted data back to its original owners, perpetrators extracted profits from personal data that had little value on the black market.[39] Today, ransomware attacks have evolved beyond encryption of data, increasingly using data theft as the primary mode of extortion.[40] After the victim company pays the ransom, perpetrators, still in possession of the company's data, can demand further payments by threatening to destroy or leak confidential or sensitive company information, or to publish the personal data of employees and customers.[41]

A number of factors have fueled the increase in the frequency and scale of ransom attacks. First, even if they are identified, cybercriminals face little risk of extradition or prosecution due to the lack of coordination among government agencies,[42] the absence of international cooperation, and the unwillingness of some countries to address cybercrime originating within their borders.[43] Second, the United States and other governments have also failed to regulate cryptocurrency, and this lack of oversight

32. Lily Hay Newman, *Apple's Ransomware Mess Is the Future of Online Extortion*, WIRED (Apr. 23, 2021, 7:00 AM), https://www.wired.com/story/apple-ransomware-attack-quanta-computer [https://perma.cc/E2KU-MW63].

33. Brian Fung, *Another Big Company Hit by a Ransomware Attack*, CNN (Aug. 11, 2021, 2:55 PM), https://www.cnn.com/2021/08/11/tech/accenture-ransomware/index.html [https://perma.cc/B8YQ-B4WQ].

34. Peter Rudegeair & Robert McMillan, *Robinhood Hack Exposes Millions of Customer Names, Email Addresses*, WALL ST. J. (Nov. 8, 2021, 8:05 PM EST), https://www.wsj.com/articles/robinhood-hack-exposes-millions-of-customer-names-email-addresses-11636408263 [https://perma.cc/E9ET-6AEX].

35. Kartikay Mehrotra & William Turton, *CNA Financial Paid $40 Million in Ransom After March Cyberattack*, BLOOMBERG (May 20, 2021, 3:57 PM EDT), https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack [https://perma.cc/VWR9-PXHC].

36. James Rundle, *Cyberattack on Payroll Provider Sets Off Scramble Ahead of Holidays*, WALL ST. J. (Dec. 17, 2021, 6:12 PM EST), https://www.wsj.com/articles/cyberattack-on-payroll-provider-sets-off-scramble-ahead-of-holidays-11639778286 [https://perma.cc/WGB7-P239].

37. Newman, *supra* note 32; *see also* Trautman & Ormerod, *Emerging Threat*, *supra* note 1, at 511.

38. Newman, *supra* note 32; Trautman & Ormerod, *Emerging Threat*, *supra* note 1, at 511.

39. WOLFF, *supra* note 31, at 70.

40. Newman, *supra* note 32 ("We're at a point where the threat actors have realized that the data itself can be used in a myriad of ways." (quoting threat analyst Brett Callow)).

41. Richardson et al., *supra* note 6, at 6; RANSOMWARE GUIDE, *supra* note 26, at 2, 13; *see* RANSOMWARE TASK FORCE, INST. FOR SEC. AND TECH., COMBATING RANSOMWARE: A COMPREHENSIVE FRAMEWORK FOR ACTION, 13 (2021) [hereinafter COMBATING RANSOMWARE].

42. GLOBAL RISKS REPORT 2022, *supra* note 2, at 9.

43. WOLFF, *supra* note 31, at 248. *But see* Press Release, White House, *supra* note 13 (highlighting counter-ransomware efforts of the National Security Council to "leverag[e] the tools of diplomacy to address safe harbors and improve partner capacity" and noting that "President Biden has directly engaged President Putin, and established the White House and Kremlin Experts Group to directly discuss and address ransomware activity").

vastly reduces the risk of detection.[44] And finally, the professionalization and commercialization of cybercrime has increased the quantity, complexity, and scale of cyberattacks.[45] In the widely used "ransomware as a service" model, a developer creates and licenses malware to an affiliate for a fixed fee or a share of the ransom payments.[46] This lowers the cost of entry for would-be perpetrators by providing the necessary technical knowledge and tools.[47]

Today, American companies are in the crosshairs of cybercriminals. Cyberattacks have evolved away from an early, high-volume approach (a profusion of low-value attempts on private individuals) and toward high-impact attacks on specific corporate targets.[48] Digitization of business systems, data, and communications, and present-day global political tensions are key causes of this shift.

First, as a result of digitization and the explosive growth of online business, corporations have become attractive targets for cyberattacks.[49] This combination of factors has proven enticing for malicious actors, who "realize[] the efficiency of targeting [company] networks for attack by stealing both corporate and consumer information."[50] Though the number of cyberattacks was already rising prior to 2020, accelerated dependence on digital systems during the COVID-19 pandemic[51] introduced new entry points for attacks on corporations due to increased automation, remote connection, and information sharing.[52] Further, with the shift of consumer interactions and transactions to the internet, personally identifiable consumer data has become a key business asset.[53] Additionally, because companies have centralized their

44. GLOBAL RISKS REPORT 2022, *supra* note 2, at 47; *see also* SEC 2023 Cybersecurity Rules, *supra* note 18, at 7 (noting that "the rapid monetization of cyberattacks" has been facilitated, in part, by "crypto-asset technology"). *But see* Alan Rappeport, Andrew E. Kramer & David E. Sanger, *The Biden Administration Is Combating Ransomware with a Crackdown on Cryptocurrency Payments*, N.Y. TIMES (Sept. 21, 2021), https://www.nytimes.com/2021/09/21/us/politics/treasury-department-combating-ransomware-cryptocurrency.html [https://perma.cc/4N9Q-6KTS].

45. *See* GLOBAL RISKS REPORT 2022, *supra* note 2, at 9.

46. COMBATING RANSOMWARE, *supra* note 41, at 16; *see also* GLOBAL RISKS REPORT 2022, *supra* note 2, at 47 ("[P]rofit-seeking groups of cyber mercenaries stand ready to provide access to sophisticated cyber-intrusion tools to facilitate [ransomware] attacks.").

47. *See* COMBATING RANSOMWARE, *supra* note 41, at 16.

48. *See* RANSOMWARE GUIDE, *supra* note 26, at 2; Brenda R. Sharton, *Ransomware Attacks Are Spiking. Is Your Company Prepared?*, HARV. BUS. REV. (May 20, 2021), https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared [https://perma.cc/UEG2-4EQZ] ("[The threat actors] understand the company's financial picture, the industry in which it operates, and how to exploit the company to maximum effect.").

49. *See* THOMAS, *supra* note 5, at 4.

50. Andrea M. Matawyshn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 145 (2005); *see also* GLOBAL RISKS REPORT 2022, *supra* note 2, at 48 ("Cyberthreat actors are also accessing higher-quality and more sensitive information from victims.").

51. GLOBAL RISKS REPORT 2022, *supra* note 2, at 9.

52. *See id.* at 9, 46; SEC 2023 Cybersecurity Rules, *supra* note 18, at 7.

53. Matawyshn, *supra* note 50, at 145.

data into information networks to increase efficiency and convenience, consumer data can be more easily targeted in an attack.[54]

Given the desire of attackers to target both corporate and consumer data, companies are not all equal in the eyes of perpetrators. A cyberattack can extract larger ransoms from data-rich corporations with higher-quality and more sensitive information.[55] A 2021 study characterized the companies most vulnerable to attacks as "larger, included in the list of Fortune 500 companies, financially less constrained, more highly valued, [with] more intangible assets. . . . [and] operating in industries that are less competitive."[56]

The shift of business interactions to digital platforms, combined with the practice of giving system access to outside vendors, has allowed cybercriminals to exploit the weaknesses of third parties' partners to launch attacks on their ultimate corporate targets.[57] Risk is increased yet further by fourth-party risks—the additional risks of the partners and associates of third parties.[58] For a cybercriminal, an attack on a vendor or other third- or fourth-party associate "downstream in the supply chain" offers key advantages—these companies are often smaller and less well-resourced and thus present softer targets with fewer cybersecurity defenses.[59]

In 2021, for example, the prominent Russian ransomware gang REvil launched a ransomware attack on Quanta Computer, a supplier to Apple.[60] On the day of a planned Apple product announcement, REvil made its own announcement, revealing that it had obtained Apple product data and schematics and would sell them to the highest bidder if Apple did not make a $50 million payment.[61] Third-party risk is not a new phenomenon. An early, memorable example is the 2013 cyberattack on Target—hackers used a phishing attack on an employee of a heating and cooling contractor to obtain remote access credentials to Target's digital systems,[62] ultimately stealing the financial and personal data of an estimated 110 million Target customers.[63]

---

54. *Id.*

55. Sharton, *supra* note 48 ("Attacks are focused on exfiltrating company information—and the more sensitive, the better.").

56. Kamiya et al., *supra* note 8, at 721.

57. *See* Matawyshn, *supra* note 50, at 171 ("[I]f one of those business partners makes even one unwise outsourcing decision which gives access to the shared data to a third entity with weak security, the consequences of a data breach by this vulnerable entity two steps removed will be felt by the initial entity."); SEC 2023 Cybersecurity Rules, *supra* note 18, at 7.

58. NAT'L ASS'N OF CORP. DIRS., CYBER THREAT ALL. & SECURITYSCORECARD, AN UPDATE ON THE STATE OF THE U.S. SECURITIES AND EXCHANGE COMMISSION'S APPROACH TO CYBER RISK 9 (2022).

59. Newman, *supra* note 32 (noting that Quanta Computer also supplies Dell and HP).

60. *Id.*

61. *Id.* As proof, REvil "released a cache of documents about upcoming, unreleased MacBook Pros" and iMac schematics. *Id.*

62. Nicole Perlroth, *Heat System Called Door to Target for Hackers*, N.Y. TIMES (Feb. 5, 2014), https://www.nytimes.com/2014/02/06/technology/heat-system-called-door-to-target-for-hackers.html [https://perma.cc/32S3-ZPBS].

63. *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1157 (D. Minn. 2014).

A second factor driving attacks on corporate targets is the emergence of a new global conflict landscape that blurs the lines between state actors and private entities.[64] Today, many corporations have a financial and symbolic value large enough to make them suitable proxies for nation-states—an attack on a high-value company can devastate a state adversary.[65] Further, because corporations have greater exposure and less protection than military targets, aggressors with fewer economic and military resources can inflict significant harm on world superpowers.[66] Given their "size, value, and influence," American companies are particularly attractive targets to enemies of the United States "who would otherwise be reticent to engage the [country] in traditional battles."[67]

Many of the largest and most visible cyberattacks on American companies have been attributed to foreign governments.[68] Though these attacks undoubtedly inflicted financial harm on their targets, the involvement of state actors suggests that they were primarily motivated by goals including "political and economic espionage, and system disruption."[69] The 2014 North Korean-backed attack on Sony Pictures, related to the studio's release of *The Interview*, a satirical movie about a CIA plot to assassinate North Korean leader Kim Jong Un, is one of the first attacks on a U.S. corporation to be attributed to a nation-state actor.[70] Yahoo was another early victim of a nation-state

64. *See* Tom C.W. Lin, *Business Warfare*, 63 B.C. L. REV. 1, 3 (2022) ("[T]his competition between and among nations and businesses has grown alarmingly and increasingly adversarial and combative as nation-states and non-state actors target specific businesses for attacks, sanctions, and recriminations with new intensity and methods." (citing J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 YALE L.J. 1020, 1024 (2020))); Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1091 (2014) ("[N]ation-states are now engaged in the long twilight struggle of espionage and hacking in cyberspace."); *see, e.g.*, Trautman & Ormerod, *Emerging Threat*, *supra* note 1, at 505–06 (discussing the North Korea-sponsored 2017 WannaCry and 2014 Sony attacks); *id.* at 534 (discussing the 2017 NotPetya attack which was linked to the Russian government).

65. Lin, *supra* note 64, at 12 ("[A] successful attack against [a high-value company] could have a devastating psychological and economic impact on an adversary. . . . The revenues and market cap of the largest technology companies in the world rival and surpass the GDP of many large nations."); *see also* SEC 2023 Cybersecurity Rules, *supra* note 18, at 7 (noting that large-scale attacks can have "systemic effects on the economy as a whole").

66. *Id.*; *see also* SCI. FORESIGHT UNIT, EUR. PARL. RSCH. SERV., HIGH-LEVEL ROUNDTABLE ON CYBERSECURITY 3 (2022) (noting attack motivations including "desire to destabilise a country, an economy, or democratic processes such as elections").

67. Lin, *supra* note 64, at 9 ("[E]nemies that could not otherwise win traditional wars of soldiers and arms with the United States, given its superpower strengths, now seek to attack American business interests directly to inflict harm on American national security and economic welfare."); *id.* at 11 ("Whereas traditional warfare tactics have often become too bloody, costly, and futile, attacks via business warfare have grown more attractive and prevalent.").

68. *Id.* at 24–25; *see also* SEC 2023 Cybersecurity Rules, *supra* note 18, at 8 ("[S]tate actors have perpetrated multiple high-profile attacks, and recent geopolitical instability has elevated such threats.").

69. WOLFF, *supra* note 31, at 259; *see also id.* at 73 (discussing North Korea's involvement in the WannaCry cyberattack and noting that "[r]ansomware appeared to have transcended its roots as a tool for financially motivated crime and developed into a more general attack model that cost its victims no less even as it brought in smaller sums for its perpetrators").

70. Trautman & Ormerod, *Emerging Threat*, *supra* note 1, at 526; *see also* David E. Sanger & Nicole Perlroth, *U.S. Said To Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES (Dec. 17, 2014),

attack. Between 2013 and 2016, multiple cyberattacks on Yahoo compromised over one billion user accounts and were subsequently attributed to Russian intelligence officers.[71] And in 2017, members of China's military attacked the credit reporting agency Equifax, stealing trade secrets and personal data from approximately 145 million individuals.[72]

B. The Harms that a Cyberattack Inflicts on a Corporation

A cyberattack triggers a broad range of harms on a corporation and can have a material effect on its revenues and share prices.[73] Most immediate and obvious among the harms inflicted by an attack are ransom payments to malicious actors and disruption of daily operations.[74] Reported 2019 ransom payments made by American companies, for example, ranged as high as 9.1% of annual revenues.[75] Other near-term impacts can include loss of trade secrets and other intellectual property, as well as exposure of confidential customer and employee data.[76]

While some harms are apparent, others are more difficult to detect and may only become clear in hindsight.[77] For example, a cyberattack blocks or limits the availability of capital, bandwidth, and other essential resources.[78] It also forces the company to dedicate employee capacity to post-attack tasks including incident response, forensic investigations, and documentation.[79] Cyberattacks also introduce the threat of state and

---

https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html [https://perma.cc/XY5D-NU73] ("It is rare for the United States to publicly accuse countries suspected of involvement in cyberintrusions."); Press Release, Off. of Pub. Affs., U.S. Dep't of Just., North Korean Regime-Backed Programmer Charged with Conspiracy To Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and [https://perma.cc/3AF4-B68R].

71. Press Release, Off. of Pub. Affs., U.S. Dep't of Just., U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts (Mar. 15, 2017), https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions/ [https://perma.cc/NS4C-UQXW].

72. Katie Benner, *U.S. Charges Chinese Military Officers in 2017 Equifax Hacking*, N.Y. TIMES (May 7, 2020), https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html [https://perma.cc/43HF-4JS4]; *see also* Criminal Indictment at 1–2, United States v. Zhiyong, No. 20-cr-00046, 2020 WL 5249460 (N.D. Ga. Jan. 28, 2020), https://www.justice.gov/opa/press-release/file/1246891/download [https://perma.cc/Q76J-XABY].

73. Thomas G. Calderon & Lei Gao, *Changes in Corporate Cybersecurity Risk Disclosures after SEC Comment Letters*, J. ACCT. & PUB. POL'Y, June 2022, at 1, 2.

74. *Handling Destructive Malware*, *supra* note 25.

75. Richardson et al., *supra* note 6, at 6.

76. Sharton, *supra* note 48; *see also* Matawyshn, *supra*, note 50, at 140 ("[C]orporate proprietary information protected solely by trade secret law could, in effect, lose all its value . . . because the information's status as a trade secret is entirely contingent upon its confidentiality."); *Id.* at 139–40 ("Certain corporate assets, such as databases of customer information and preferences, are valuable only because of their confidentiality.").

77. Kosseff, *supra* note 4, at 990–93.

78. Matawyshn, *supra* note 50, at 142 (highlighting the need to cover fines, court costs, attorneys' fees, settlement costs, compliance mechanisms, settlement agreements, and court decisions).

79. *Id.*

federal regulatory fines and the possibility of civil claims brought under state laws.[80] When an attack becomes public, it may also cause brand damage, which can reduce the market value of a company's products.[81]

Another less apparent harm is reputational damage, which can become a "reputational loss" when stakeholders demand more favorable transactional terms (e.g., loan terms) to account for their increased financial risk.[82] The effects of reputational loss can be substantial, including negative impacts on sales growth, return on assets, and cash flow; decreased credit ratings; and lower ratios of net worth to assets.[83] The cyberattacks suffered by Yahoo provide a prime example of the effects of reputational loss on shareholders.[84] Following two attacks and the company's failure to disclose them, Verizon renegotiated its asset purchase deal to cut $350 million from the price it would pay.[85] The full amount of this loss was passed directly on to Yahoo shareholders.[86]

Cyber incidents also create volatility in stock prices, which, in turn, has a tangible effect on shareholder wealth.[87] One investigation found that companies experienced a drop in stock price following the announcement of a data breach and saw persistently lower stock prices for several years.[88] Notably, the study showed that the market punished more heavily those data breaches that could have been avoided with reasonable precautions.[89] A 2021 study found that while the out-of-pocket costs of a cyberattack were significant, they made up only a small portion of the average $495

80. *See* Edward A. Morse, Vasant Raval & John R. Wingender, Jr., *SEC Cybersecurity Guidelines: Insights into the Utility of Risk Factor Disclosures for Investors*, 73 BUS. LAW. 1, 1 (2017) [hereinafter Morse et al., *Cybersecurity Guidelines*]; SEC 2023 Cybersecurity Rules, *supra* note 18, at 7 (noting that litigation risks are among the increasing costs of cyberattacks); *infra* Part II.E (discussing statutory and regulatory law addressing cybersecurity and the associated liability).

81. *See* Kosseff, *supra* note 4, at 990–93 (detailing harms of the 2014 Sony Pictures hack); Matawyshn, *supra* note 50, at 140 (noting that vulnerability decreases investments in brand identity, due to breached promises of data care); Kamiya et al., *supra* note 8, at 721.

82. Kamiya et al., *supra* note 8, at 720; *see also* Virginia Harper Ho, *Risk-Related Activism: The Business Case for Monitoring Nonfinancial Risk*, 41 IOWA J. CORP. L. 647, 665 (2016) [hereinafter Harper Ho, *Risk-Related Activism*] ("One of the consistent findings on risk effects is that firms with strong monitoring and management of nonfinancial risks enjoy a lower cost of equity and cheaper debt financing . . . [and] share prices should reflect the fact that discounting by a lower cost of capital increases the net present value of the firm's earnings."); *see also* SEC 2023 Cybersecurity Rules, *supra* note 18, at 7 (noting that reputational damage is among the increasing costs of cyberattacks).

83. Kamiya et al., *supra* note 8, at 720.

84. See *supra* note 71 and accompanying text regarding the 2013-2016 cyberattacks on Yahoo.

85. Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Breach*, 66 AM. U. L. REV. 1231, 1285 (2017) [hereinafter Trautman & Ormerod, *Cybersecurity Standard of Care*].

86. *Id.*

87. Kamiya et al., *supra* note 8, at 720; Morse et al., *Cybersecurity Guidelines*, *supra* note 80, at 1.

88. Edward A. Morse, Vasant Raval & John R. Wingender Jr., *Market Price Effects of Data Security Breaches*, 20 INFO. SEC. J. 263, 270 (2011) [hereinafter Morse et al., *Market Price Effects*] (examining 2000–2010 reported breaches).

89. *Id.*

million shareholder value loss occurring in the three-day window after a cyberattack[90]—the greater share of value loss was attributed to reputational loss.[91]

C. *The Challenges of Cybersecurity Planning*

Understanding and addressing cyber-threats is part of the cost of doing business,[92] because a company's survival depends on the protection of its critical information and its technology infrastructure.[93] Responses to cyber-threats fall under the umbrella term "cybersecurity."[94] A comprehensive corporate cybersecurity plan includes both proactive and responsive strategies to reduce the chance of attacks, quickly detect an intrusion, respond effectively, and recover from a worst-case scenario.[95]

An emerging cybersecurity standard of care takes a process-oriented approach and emphasizes ongoing review and adjustment.[96] Nonetheless, there is no one-size-fits-all

---

90. Kamiya et al., *supra* note 8, at 721 (representing a 0.84% average shareholder value loss; if the attack included loss of personal financial information value loss averaged 1.09%). The study looked at disclosed cyberattacks on public corporations from 2005 to 2017. *Id.* at 720, 727.

91. *Id.* at 737; *see also* Morse et al., *Cybersecurity Guidelines*, *supra* note 80, at 2 ("[E]rosion of customer goodwill, reduced investor confidence in management's ability to secure the firm's assets, and exposure to transaction costs associated with resolving claims may explain negative effects on stock prices.").

92. Robert Kolasky, *Foreword* to INTERNET SEC. ALL. & NAT'L ASSOC. OF CORP. DIRS., CYBER-RISK OVERSIGHT 2020 KEY PRINCIPLES AND PRACTICAL GUIDANCE FOR CORPORATE BOARDS 4 (2020), http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf (discussing the importance of robust risk-management practices, including "knowing your major risks, understanding the size of your attack surface, assessing the criticality of your digital infrastructure based on the type of business processes they support, conducting inventories of connected users and devices, and then using this awareness to harden systems and add resilience in a targeted and prioritized manner"); *see also* Harper Ho, *Risk-Related Activism*, *supra* note 82, at 655 ("Like other nonfinancial risk, operational risks . . . are inherent in any business and cannot be hedged or completely eliminated, and . . . they can also affect financial risk."); Kamiya et al., *supra* note 8, at 720 ("Firms could choose not to be exposed to cyber risk, but they would not be competitive doing so and likely would not be able to function.").

93. *See* Kosseff, *supra* note 4, at 997 (emphasizing "the need to protect not only data, but also the systems on which data are stored and the networks on which data are transmitted").

94. Div. of Corp. Fin., *Corporate Finance Disclosure Guidance: Topic No. 2, Cybersecurity*, SEC (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [https://perma.cc/928D-FXQE] ("Cybersecurity is the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access.").

95. *Shields Up*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/shields-up [https://perma.cc/ZBU7-2JLY] (last visited Nov. 22, 2023); *see, e.g.*, CYBERSECURITY AND RESILIENCY OBSERVATIONS, *supra* note 5, at 2 (noting "practices in the areas of governance and risk management, access rights and controls, data loss prevention, mobile security, incident response and resiliency, vendor management, and training and awareness"); Kolasky, *supra* note 92, at 5 (discussing basic cybersecurity hygiene, including "backing up systems, patch management, and network segmentation"); *2021 Top Malware Strains, supra* note 23 (listing key practices, including patching known exploited vulnerabilities, enforcing multifactor authentication, making offline backups of data, training end-users about social engineering and phishing).

96. Trautman & Ormerod, *Cybersecurity Standard of Care*, *supra* note 85, at 1241–42 (2017); *see also, e.g.*, WILLIAM C. BARKER, WILLIAM FISHER, KAREN SCARFONE & MURUGIAH SOUPPAYA, NAT'L INST. OF STANDARDS AND TECH., DEP'T OF COM., RANSOMWARE RISK MANAGEMENT: A CYBERSECURITY FRAMEWORK PROFILE (2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf [https://perma.cc/5K8Q-9SUL] (Department of Commerce guidelines for ransomware prevention, response, and recovery). *But see*

approach for companies, and cybersecurity risk planning presents a substantial challenge. Cybersecurity decisions are highly case specific and depend on the company's function, infrastructure, and data assets, among other factors.[97] Recommended practices and solutions are constantly changing as threats evolve.[98] The current reality is that companies are faced with an "excess of security advice and services, coupled with a lack of reliable, empirical data on which controls and techniques are most effective at preventing intrusions."[99]

American companies receive little cybersecurity direction from the federal government, either in the form of actionable recommendations[100] or well-defined liability regimes.[101] As cybersecurity policy expert Josephine Wolff observes, "[T]he vague nature of government cybersecurity guidance adds to the uncertainty that institutions face when forced to make concrete decisions about how to define the scope of their responsibility for protecting computer systems and what tools to use for that purpose."[102] She points out that the Federal Trade Commission (FTC), for example, does not identify any specific cybersecurity practices companies can implement to avoid liability in the case of a cyberattack, "in part because [the FTC does] not know which controls are most effective—they have no way to measure that."[103]

D. The Role of the Board of Directors in Cybersecurity Oversight

Corporate law holds boards of directors accountable to preserve and grow value for investors,[104] and oversight of risk management is an essential component of a board's role.[105] Along with the many other corporate risks they address, directors have a responsibility to protect the company from the immediate and longer-term harms of a cyberattack.[106] Though it is not possible to eliminate all danger, anticipating, preparing

---

WOLFF, *supra* note 31, at 226 (referring to an "amorphous set of 'best practices' that are almost never explicitly codified until after a breach").

97. *See* WOLFF, *supra* note 31, at 227.

98. *Id.*

99. *Id.* at 226.

100. *Id.* at 227.

101. *Id.* at 279.

102. *Id.* at 227.

103. *Id.* at 252.

104. Kolasky, *supra* note 92, at 6 ("As corporate fiduciaries, boards of directors are responsible for . . . identification and planned response to enterprise-wide risks impacting the company and its value to stakeholders and shareholders.").

105. Harper Ho, *Risk-Related Activism*, *supra* note 82, at 655; *see also id.* at 663–64 ("Risk management is the process of identifying, monitoring, reporting and responding to the range of financial, operational and strategic risks that firms face. . . . It is . . . considered integral to firm strategy and a core governance function.").

106. *See* Luis Aguilar, SEC Comm'r, Speech at the New York Stock Exchange Cyber Risks and the Boardroom Conference: Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (June 10, 2014), https://www.sec.gov/news/speech/2014-spch061014laa [https://perma.cc/6LYJ-385Q] ("[E]nsuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities."); COUNCIL OF INST. INVS., CORPORATE GOVERNANCE POLICIES § 2.7, at 7 (2022) [hereinafter CII, GOVERNANCE POLICIES], https://www.cii.org/files/09_21_22_corp_gov_

for, and managing risk can contribute to a company's long-term value by reducing future losses due to "enforcement actions, legal claims, and other negative risk events."[107] To accomplish this, directors must set priorities and allocate resources and expertise to support a cybersecurity risk management strategy that is both proactive and responsive.[108] Further, under the SEC's new Cybersecurity Rules, directors are tasked with ensuring that disclosures accurately and fully portray the company's cyber-risk to investors and securities markets.[109] Though there is a compelling argument for increasing the awareness of cybersecurity risk management in corporate boardrooms, there are a number of trade-offs and conflicting incentives that complicate decision-making around corporate cybersecurity.

Boards can address cybersecurity risks by hiring a chief information security officer,[110] directing the purchase of cyber insurance,[111] and engaging outside service providers for continuous threat monitoring.[112] However, these investments are expensive[113] and ultimately require a "trade-off between the benefit of reducing the risk [that profit volatility] imposes on stakeholders and the cost of doing so."[114] And because an investment in cybersecurity will likely reduce or eliminate attacks, stakeholders may perceive a reduced threat and feel that the company is overinvesting in cybersecurity.[115]

Given the costs and the risk analysis, boards may decide to forgo cybersecurity investments and instead focus on managing the consequences of an attack.[116] Though cyberattack costs can be significant, market and business factors may not adequately incentivize cybersecurity investments. Decision-makers may believe that the

policies.pdf (noting that "directors share ultimate responsibility for effective risk oversight" for material industry and systemic risks including cybersecurity); Michelle Lowry, Anthony Vance & Marshall D. Vance, Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity 7 (Dec. 28, 2021) (unpublished manuscript), https://ssrn.com/abstract=4002794 [https://perma.cc/W8G5-VYSD].

107. Harper Ho, *Risk-Related Activism*, *supra* note 82, at 664.

108. *See* Jared Ho, *Corporate Boards: Don't Underestimate Your Role in Data Security Oversight*, FTC (Apr. 28, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/corporate-boards-dont-underestimate-your-role-data-security-oversight [https://perma.cc/NEC9-D3YK]; Tracy Stewart, Council of Inst. Invs., Comment Letter on Proposed Rule Regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, at 2 (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128381-291284.pdf [https://perma.cc/7F2G-TGVT].

109. Stewart, *supra* note 108, at 2.

110. Henk Berkman, Jonathan Jona, Gladys Lee & Naomi Soderstrom, *Cybersecurity Awareness and Market Valuations*, 37 J. ACCT. & PUB. POL'Y 508, 509 (2018).

111. *Id.*

112. *See* NAT'L ASS'N OF CORP. DIRS. ET AL., *supra* note 58, at 5–6.

113. *See* Kamiya et al., *supra* note 8, at 723.

114. *Id.* at 722; *see also* Kolasky, *supra* note 92, at 5 ("[E]fforts need to be made to . . . evaluate incidents and controls in terms of their impact on business outcomes . . . to better evaluate the merit of additional investments in cyber controls and other forms of risk management.").

115. *See* Morse et al., *Market Price Effects*, *supra* note 88, at 272 (noting that cost and value can be balanced "by including qualitative variables in the incentive plans of the CEO, CIO, CRO, and CISO, thus rewarding them for the absence of breaches over a period of time").

116. Musaib Ashraf, *The Role of Peer Events in Corporate Governance: Evidence from Data Breaches*, ACCT. REV., Mar. 2022, at 1.

out-of-pocket costs of a potential attack will constitute only a fraction of the company's annual revenues.[117] Further complicating the cost-benefit analysis of cybersecurity investments for corporate decision-makers, cyberattack expenses can often be at least partially reimbursed by insurance.[118] In addition, existing regulatory penalties are not yet significant enough to encourage companies to forego potential revenue in order to invest in compliance.[119] A 2021 study, for example, estimated regulatory fines resulting from a cyberattack at only $1.02 million.[120]

The threat of investor claims for breach of oversight duty is also unlikely to substantially affect decision making around cybersecurity investments.[121] Delaware's business judgment rule gives substantial deference to boards in monitoring and responding to risk, and the high standard for liability requires an intentional disregard of fiduciary duties.[122] The Delaware Court of Chancery itself has observed that director liability based on the duty of oversight "is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment."[123]

E. SEC Cybersecurity Regulation

The SEC has begun to insert itself in this environment of cybersecurity risk, asserting that oversight in this area is integral to the Commission's work to protect

---

117. Kosseff, *supra* note 4, at 1004 (citing Benjamin Dean, *Why Companies Have Little Incentive To Invest in Cybersecurity*, THE CONVERSATION (Mar. 4, 2015, 2:26 PM), http://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570 (asserting that "[t]he questionable efficacy of coercive cybersecurity regulation is traceable, in part, to the relatively low costs of penalties for large companies," as evidenced by the fact that cyberattacks on Sony Pictures, Target, and Home Depot cost the companies less than one percent of their annual revenues).

118. Kosseff, *supra* note 4, at 1004. *But see* Paul Ferrillo, Bob Zukis & Christophe Veltsos, *Proposed SEC Cyber-Rules: A Game-Changer for Public Companies*, HARV. L. SCH. F. ON CORP. GOVERNANCE (April 11, 2022), https://corpgov.law.harvard.edu/2022/04/11/proposed-sec-cyber-rules-a-game-changer-for-public-companies/ [https://perma.cc/25EK-DC9K] ("Whereas corporate leadership may have felt that cyber insurance effectively transferred the majority of their risk exposure to a third-party, the reality of the expanding impacts of cyber risk means that issuers are primarily self-insured for the significant majority of the cyber risks and costs that they face.").

119. Kosseff, *supra* note 4, at 1004 ("[O]ur legal system has not yet created adequate incentives for individual companies to take the necessary—and sometimes costly—steps to reduce the likelihood of cybersecurity attacks.").

120. Kamiya et al., *supra* note 8, at 734.

121. Harper Ho, *Risk-Related Activism*, *supra* note 82, at 659.

122. *See id.* ("Absent willful disregard for fiduciary duties, such a complete failure to implement a compliance system or a failure to respond to 'red flags' as they arise, the business judgment rule ensures substantial deference to boards in implementing a compliance system, and in monitoring and responding to risk events." (citing Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006))). Under Delaware's business judgement rule, "the judgment of a properly functioning board will not be second-guessed and '[a]bsent an abuse of discretion, that judgment will be respected by the courts.' 'To avoid application of the deferential business judgment standard, the plaintiff must produce evidence that rebuts the business judgment presumption.'" *In re* KKR Fin. Holdings LLC S'holder Litig., 101 A.3d 980, 989–90 (Del. Ch. 2014) (first quoting Orman v. Cullman, 794 A.2d 5, 20 (Del. Ch. 2002); and then quoting eBay Domestic Holdings, Inc. v. Newmark, 16 A.3d 1, 36–37 (Del. Ch. 2010)).

123. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967 (Del. Ch. 1996).

investors and ensure the integrity of financial markets.[124] The SEC's primary tool in regulating corporate cybersecurity is its public disclosure framework, first established by Congress in 1934.[125] This Part will examine the throughline that begins with the original rationale for corporate disclosures and extends all the way to the SEC's 2023 Cybersecurity Rules. It details the foundations and intent of the disclosure framework and then considers several key SEC actions in the timeline leading up to the 2023 finalization of the Rules.

1. The SEC Disclosure Framework

The Securities Act of 1934 ("Exchange Act") created the SEC and empowered it with broad authority to regulate the securities industry, including all publicly traded companies.[126] The Exchange Act was designed, in large part, to protect shareholders of American companies.[127] As of the writing of this Comment, the Exchange Act gives the SEC oversight of all corporations that are listed on a U.S. exchange, as well as all corporations that have $10 million in assets and either two thousand shareholders or five hundred shareholders who are not accredited investors.[128]

The SEC's "long-standing three-part mission [is] to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation."[129] To further the aim of protecting shareholders, the Exchange Act specified that the SEC would require reporting, or "disclosure," to provide information to investors about companies in which they are investing.[130] This requirement is grounded in the basic assertion that "[t]imely disclosure of relevant information allows investors to make informed decisions about their investments and induces confidence from the investment community."[131] In 1934, Congress prescribed only a skeletal framework for disclosure

124. *See* Mary Jo White, SEC Chair, Opening Statement at SEC Roundtable on Cybersecurity, SEC (Mar. 26, 2014), https://www.sec.gov/news/statement/statement-3-26-14-mjw [https://perma.cc/S4PZ-2JJN].

125. *See Investor Bulletin: An Introduction to the U.S. Securities and Exchange Commission – Rulemaking and Laws*, SEC, https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_rulemaking [https://perma.cc/QWL6-DRHP] (last updated Feb. 6, 2017).

126. *Id.*

127. Cynthia A. Williams, *The Securities and Exchange Commission and Corporate Social Transparency*, 112 HARV. L. REV. 1197, 1226–27 (1999).

128. 15 U.S.C. § 78l(g)(1)(A); *see also* Accredited Investor Definition, Securities Act Release No. 10,824, Exchange Act Release No. 89,669, 85 Fed. Reg. 64234, 64276–78 (Oct. 9, 2020) (codified at 17 CFR pts. 230, 240).

129. SEC, STRATEGIC PLAN: FISCAL YEARS 2022–2026, at 7 (2022), https://www.sec.gov/files/sec_strategic_plan_fy22-fy26.pdf https://perma.cc/5GWH-CLGB].

130. Securities Exchange Act of 1934, Pub. L. No. 73-291, ch. 404, § 13, 48 Stat. 881, 894 (codified as amended at 15 U.S.C. §§ 78m(a)(2)) ("Every issuer of a security registered on a national securities exchange shall file the information, documents, and reports below specified with the exchange . . . in accordance with such rules and regulations as the Commission may prescribe as necessary or appropriate for the proper protection of investors and to insure fair dealing in the security . . . .").

131. Morse et al., *Cybersecurity Guidelines*, *supra* note 80, at 5; *see also* Lori J. Schock, Acting Dir., Off. of Inv. Educ. and Assistance, SEC, Feedback from Individual Investors on Disclosure, Address to Vanguard & Villanova University Center for Marketing & Public Policy Research (Jan. 19, 2007), https://www.sec.gov/news/speech/2007/spch011907ljs.htm [https://perma.cc/YX9V-JKKR] ("[T]he federal securities laws are derived from one simple and straightforward concept: all investors, whether large

and gave the SEC broad authority to promulgate the disclosure rules.[132] Today, SEC rules require companies to make annual and periodic disclosures to investors about business operations, management, financial conditions, and risk factors, among other details.[133]

As reflected in the SEC's second mission objective, "maintain[ing] fair, orderly, and efficient markets,"[134] Congress also saw disclosure as a way "to promote market efficiency so that the prices of securities would more accurately reflect the underlying values of the securities."[135] In 2019, then-SEC Division of Corporation Finance Director William Hinman highlighted the importance of this objective: "Robust disclosure decreases information asymmetries and is the foundation of reliable price discovery. When investors have confidence that they are receiving full and transparent disclosure, markets operate more efficiently and the cost of capital is reduced."[136]

Finally, disclosure is a key means of fulfilling the SEC's commitment to "facilitate capital formation."[137] The SEC has asserted that disclosure requirements are designed to "maintain[] investor confidence in the reliability of public company information, in order to, among other things, encourage capital formation."[138]

Disclosure is a year-round process[139] designed to elicit "timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision."[140] In addition to quarterly and annual

institutions or private individuals, should have access to certain basic facts about an investment prior to buying it, and so long as they hold it.").

132. Morse et al., *Cybersecurity Guidelines*, *supra* note 80, at 4; SEC, REPORT ON REVIEW OF DISCLOSURE REQUIREMENTS OF REGULATION S-K 8–9 (2013), https://www.sec.gov/news/studies/2013/reg-sk-disclosure-requirements-review.pdf [https://perma.cc/9U87-54HV].

133. *Exchange Act Reporting and Registration*, SEC, https://www.sec.gov/education/smallbusiness/goingpublic/exchangeactreporting [https://perma.cc/S3MV-TGAC] (last updated Apr. 6, 2023); *see also* 15 U.S.C. § 78b.

134. See *supra* note 129 and accompanying text discussing the SEC's three-part mission.

135. Williams, *supra* note 127, at 1210; *see also* H.R. REP. 73-1383, at 11 (1934) ("The idea of a free and open public market is built upon the theory that competing judgments of buyers and sellers as to the fair price of a security brings about a situation where the market price reflects as nearly as possible a just price. . . . [T]he hiding and secreting of important information obstruct the operation of the markets as indices of real value.").

136. William Hinman, Dir., Div. of Corp. Fin., SEC, Applying a Principles-Based Approach to Disclosing Complex, Uncertain and Evolving Risks, Remarks at the 18th Annual Institute on Securities Regulation in Europe (Mar. 15, 2019), https://www.sec.gov/news/speech/hinman-applying-principles-based-approach-disclosure-031519 [https://perma.cc/SNB7-4UXC].

137. See *supra* note 129 and accompanying text discussing the SEC's three-part mission.

138. SEC, REPORT ON REVIEW OF DISCLOSURE REQUIREMENTS OF REGULATION S-K 94–95 (2013), https://www.sec.gov/news/studies/2013/reg-sk-disclosure-requirements-review.pdf [https://perma.cc/ZRT3-5YVS].

139. Williams, *supra* note 127, at 1207.

140. Div. of Corp. Fin., *supra* note 94.

reports,[141] companies must disclose events that would be of *material importance* to investors.[142]

This materiality standard is central to disclosure and is intended to "filter out essentially useless information that a reasonable investor would not consider significant."[143] The SEC relies on the materiality standard articulated by the Supreme Court in two cases, *TSC Industries v. Northway* and *Basic v. Levinson.*[144] *TSC Industries* established that a fact is material if it "would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."[145] Additionally, *Basic v. Levinson* established that materiality requires a fact-specific inquiry, where no single fact is determinative, and specified that the analysis requires consideration of the "probability that the event will occur and the anticipated magnitude of the event in light of the totality of company activity."[146]

The SEC reviews each company's disclosures at least once every three years.[147] If a disclosure is found to be deficient or unclear, the SEC may send a comment letter requesting amendments or additions[148] and may also conduct an investigation.[149] This can lead to an enforcement action,[150] including the possibility of an administrative proceeding or litigation in federal court.[151]

---

141. 17 C.F.R. §§ 249.308a, 249.310 (2023); *Form 10-Q*, SEC, https://www.sec.gov/about/forms/form10-q.pdf [https://perma.cc/E3FY-PHK5] (last visited Nov. 22, 2023); *Form 10-K*, SEC, https://www.sec.gov/about/forms/form10-k.pdf [https://perma.cc/PSR3-UEVV] (last visited Nov. 22, 2023).

142. *See* § 249.308 (Form 8-K required pursuant to §§ 240.13a-11, 240.15d-11); *Form 8-K*, SEC, http://www.sec.gov/about/forms/form8-k.pdf [https://perma.cc/L9K8-FYQQ] (last visited Nov. 22, 2023) (triggers include acquisitions, bankruptcy, and resignation of directors).

143. Basic v. Levinson, 485 U.S. 224, 234 (1988) (citing TSC Indus. v. Northway, 426 U.S. 438, 448–49 (1976)).

144. *See id.*; *TSC Indus*, 426 U.S. 438; Paul Munter, *Assessing Materiality: Focusing on the Reasonable Investor When Evaluating Errors*, SEC n.4 (March 9, 2022), https://www.sec.gov/news/statement/munter-statement-assessing-materiality-030922 [https://perma.cc/G2RH-XY7X]; SEC 2023 Cybersecurity Rules, *supra* note 18, at 14.

145. *TSC Indus*., 426 U.S. at 449.

146. *Basic*, 485 U.S. at 238 (citing SEC v. Texas Gulf Sulphur Co., 401 F.2d 833, 849 (2d Cir. 1968)).

147. *See* 15 U.S.C. § 7266 (added by Sarbanes-Oxley Act, Pub. L. No. 107-204, § 408, 116 Stat. 745, 790 (2002)); Stephen V. Brown, Xiaoli Tian & Jennifer Wu Tucker, *The Spillover Effect of SEC Comment Letters on Qualitative Corporate Disclosure: Evidence from the Risk Factor Disclosure*, 35 CONTEMP. ACCT. RSCH. 622, 626 (2018) ("In the aftermath of the Enron accounting scandal, one of the primary complaints against the SEC was that it had not reviewed Enron's financial statements since 1997. Shortly thereafter, section 408 of SOX began requiring the SEC to conduct some level of review of each publicly listed company at least once every three years." (citation omitted)).

148. Zahn Bozanica, J. Richard Dietrich & Bret A. Johnson, *SEC Comment Letters and Firm Disclosure*, 36 J. ACCT. & PUB. POL'Y 337, 340 (2017) (comments may request supplemental information, request a revision to future filings, or request an amendment of the filing).

149. Brown et al., *supra* note 147, at 623.

150. *Id.*

151. *About the Division of Enforcement*, SEC (Aug. 2, 2007), https://www.sec.gov/enforce/Article/enforce-about [https://perma.cc/8LKS-K3EB].

Though the SEC has continuously reiterated the importance of cybersecurity,[152] until the finalization of the Cybersecurity Rules in 2023, the Commission did not institute any mandatory rule that would require all reporting companies to regularly disclose cybersecurity information.[153] Instead, the Commission used a combination of existing rules and guidance to encourage disclosures of cyber-events, responses, and risks that would be material to investors, in light of the company's vulnerability, threat experience, and cybersecurity practices.[154]

2. 2011: The SEC Division of Corporation Finance Staff Issues Cybersecurity Guidance

In May 2011, five senators asked the SEC to issue guidance regarding cyber-risk disclosures under existing regulations.[155] Four months later, the staff of the SEC Division of Corporation Finance released guidance discussing its views on disclosure of cyber-risk and cyber-incidents.[156] Acknowledging that "no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents," the staff guidance was intended to assist companies in determining what information, if any, should be designated as material, given the company's particular circumstances.[157]

The guidance identified the primary areas of the annual disclosure form where companies have an obligation to discuss cyber-risk and cybersecurity. In the risk factor disclosure, for example, companies were urged to "disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky."[158] The guidance stated that in the section commonly known as the "MD&A," Management's Discussion and Analysis of Financial Condition and Results of Operations, companies should address cybersecurity risks and events if the costs or other consequences would likely have a material effect on financial conditions or outcomes.[159] The guidance also emphasized that "all available relevant information" must be used in determining whether risk factor disclosure is required and specified factors including prior or threatened events, severity and frequency of events, probability of events, degree of risk, costs and other consequences

152. *See* CYBERSECURITY AND RESILIENCY OBSERVATIONS, *supra* note 5, at 1 ("The SEC has focused on cybersecurity issues for many years, with particular attention to market systems, customer data protection, disclosure of material cybersecurity risks and incidents, and compliance with legal and regulatory obligations under the federal securities laws.").

153. *See* Trautman & Ormerod, *Cybersecurity Standard of Care*, *supra* note 85, at 1237 (discussing previous SEC guidance on the disclosure of cybersecurity information).

154. SEC Staff Interpretation No. 38, 83 Fed. Reg. 8166 (Feb. 26, 2018).

155. Letter from U.S. Sens. John D. Rockefeller IV, Robert Menendez, Sheldon Whitehouse, Mark Warner & Richard Blumenthal to Mary Schapiro, SEC Chair (May 11, 2011), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e (noting a 2009 Hiscox Insurance survey finding that fewer than half of Fortune 500 companies were disclosing their cybersecurity risk).

156. Div. of Corp. Fin., *supra* note 94.

157. *Id.*

158. *Id.*; 17 C.F.R. § 229.105 (2023).

159. Div. of Corp. Fin., *supra* note 94.

of misappropriation of data, operational disruption, and adequacy of preventative actions.[160]

While the 2011 staff guidance aimed to encourage robust cybersecurity disclosures, it left open significant space for companies to make their own determinations about what was required.[161] Importantly, it did not clarify the application of the materiality standard to the MD&A disclosure.[162] Additionally, while the guidance cautioned against "generic 'boilerplate' disclosure," it also stated that the rules did not require disclosures that "would compromise a registrant's cybersecurity."[163] As observed by scholars, the guidance "suggests that obfuscation through generalization is expected."[164]

The most important limitation of the 2011 guidance is the fact that it was issued only by the staff of the Division of Corporation Finance.[165] "[It was] not a rule, regulation, or statement of the Securities and Exchange Commission" and "the Commission . . . neither approved nor disapproved its content."[166] As such, this guidance was not legally binding.[167] As securities laws include no general requirement to disclose all material facts that shareholders would presumably like to know about, "[t]here is no affirmative duty to disclose facts simply because they are material."[168] As one observer noted, "silence is an option under federal securities laws unless disclosure is required."[169]

3. 2014: The SEC Asserts Its Authority for Cybersecurity Oversight

In 2014, the SEC hosted a roundtable discussion to gather private sector input on the Commission's approaches to cybersecurity regulation.[170] In his opening remarks, Luis Aguilar, then-SEC Commissioner, addressed the appropriateness of the SEC's

---

160. *Id.*

161. Jill E. Fisch, *Making Sustainability Disclosure Sustainable*, 107 GEO. L.J. 924, 955–56 (2019) ("[B]ecause [they are] premised on a materiality determination by management, the disclosures offer management substantial discretion that is often exercised in favor of failing to disclose. Even well-meaning insiders may evaluate the materiality standard differently.").

162. *See id.* at 954 ("[T]he vague and flexible standard makes the [MD&A] requirement difficult for issuers to comply with.").

163. Div. of Corp. Fin., *supra* note 94 ("[R]egistrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence.").

164. Morse et al., *Cybersecurity Guidelines*, *supra* note 80, at 9.

165. *Id.* at 12 ("[T]he fact that the 2011 Cybersecurity Guidance does not rise to the level of a rule requiring disclosure is highly significant.").

166. Div. of Corp. Fin., *supra* note 94.

167. *Guidance Updates*, SEC (Nov. 14, 2022), https://www.sec.gov/investment/im-guidance-updates.html [https://perma.cc/9NTX-NCGU]; *Staff Interpretations*, SEC (Jan. 8, 2021), http://www.sec.gov/interps.shtml [https://perma.cc/RHX4-AX83].

168. Morse et al., *Cybersecurity Guidelines*, *supra* note 80, at 11 (quoting THOMAS LEE HAZEN, TREATISE ON THE LAW OF SECURITIES REGULATION § 12.19 (Supp. 2017)).

169. *Id.* at 2 n.5.

170. *Cybersecurity Roundtable*, SEC (July 11, 2019), https://www.sec.gov/spotlight/cybersecurity-roundtable.shtml [https://perma.cc/LF5N-MD6E].

jurisdiction in the area of corporate cybersecurity, asserting that cyber-regulation was grounded in the history of the SEC's congressional mandate: "Cyber-attacks aimed at [public companies and capital markets] can have devastating effects on our economy, on individual consumers, and on the markets and investors that the SEC was created to safeguard."[171] Then-SEC Chair Mary Jo White reinforced this message, in her address at the event. She drew an explicit connection between cybersecurity oversight and the SEC's mission objectives,[172] stating that SEC cybersecurity regulation was focused on "the integrity of our market systems, customer data protection, and disclosure of material information."[173]

4. 2018: The SEC Itself Issues Cybersecurity Guidance for the First Time

In 2018, "[i]n light of the increasing significance of cybersecurity incidents," the Commission itself issued a rule interpretation and expanded on the 2011 staff guidance.[174] Though the 2018 SEC guidance did have the weight of an official Commission interpretation, it too was neither a law nor a regulation.[175] Further, while the SEC commissioners unanimously approved the 2018 guidance, many of them felt that it could have been issued as a binding requirement.[176]

The 2018 rule interpretation added guidance regarding the inclusion of cybersecurity in the analysis of a company's disclosure controls and procedures[177] and addressed insider trading based on material non-public information related to a cyber event.[178] It also discussed the role of corporate boards in cybersecurity oversight, stating that disclosures should include information to enable "investors to assess how a board of directors is discharging its risk oversight responsibility."[179] This guidance was grounded in the SEC's position that "the development of effective disclosure controls and procedures is best achieved when a company's directors . . . are informed about the cybersecurity risks and incidents that the company has faced or is likely to face."[180]

171. Luis A. Aguilar, SEC Comm'r, Statement at SEC Roundtable on Cybersecurity: The Commission's Role in Addressing the Growing Cyber-Threat (March 26, 2014), https://www.sec.gov/news/public-statement/2014-statement032614-laa#_ednref1 [https://perma.cc/EWK9-YHGM].

172. See *supra* note 129 and accompanying text discussing the SEC's three-part mission.

173. White, *supra* note 124.

174. SEC Staff Interpretation No. 38, *supra* note 154, at 6.

175. *See* Calderon & Gao, *supra* note 73, at 2.

176. *Id.* ("For example, SEC Commissioner Kara Stein . . . called for making the occurrence of a cyber attack a mandatory Form 8-K reporting event.").

177. *See* SEC Staff Interpretation No. 38, *supra* note 154, at 18 ("Companies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications . . . .").

178. *See id.* at 5 ("We recognize that many companies have adopted preventative measures to address the appearance of improper trading and we encourage companies to consider such preventative measures in the context of a cyber event.").

179. *Id.* at 18.

180. *Id.* at 4–5.

5. Enforcement Actions Reiterate the SEC's Cybersecurity Focus

Beginning in 2018, the SEC undertook a number of enforcement actions that both signaled its prioritization of cybersecurity disclosures and, to some extent, communicated to companies how the SEC would evaluate cybersecurity disclosures in light of the 2018 guidance. These enforcement actions also evidenced the fact that there were problems with compliance under the 2011 and 2018 guidance.[181]

The SEC brought its first cybersecurity disclosure action in 2018, against Yahoo, alleging disclosure failures following the 2013–2016 breaches.[182] The SEC stated that "Yahoo senior management . . . did not properly assess the scope, business impact, or legal implications of the breach, including how and where the breach should have been disclosed in Yahoo's public filings."[183] Yahoo ultimately agreed to a $35 million settlement with the SEC.[184]

In 2021, the SEC issued an administrative order against the educational publishing company Pearson, for omissions and misleading statements related to a cyberattack that compromised its data.[185] Though Pearson had characterized the cyberattack as *hypothetical* in its disclosure, the company was in fact aware that the attack had actually occurred.[186] Other recent enforcement actions include charges of deficient cybersecurity procedures[187] and cybersecurity disclosure controls failures.[188]

6. 2022–2023: The SEC Proposes and Finalizes New Cybersecurity Rules

In March 2021, "[i]n response to serious data breaches of various companies," a bipartisan group of lawmakers introduced the Cybersecurity Disclosure Act of 2021 ("CDA").[189] In his introductory remarks, Senator Jack Reed stated, "Investors and customers deserve a clear understanding of whether publicly traded companies are prioritizing cybersecurity and have the capacity to protect investors and customers from

181. *See* Virginia Harper Ho, *Nonfinancial Risk Disclosure and the Costs of Private Ordering*, 55 AM. BUS. L.J. 407, 429–30 (2018) [hereinafter Harper Ho, *Nonfinancial Risk Disclosure*].

182. Altaba Inc., Securities Act Release No. 10,485, Exchange Act Release No. 83,096, 2018 WL 1919547 (Apr. 24, 2018).

183. *Id.* at *4. Yahoo's agreement to a $29 million settlement in the derivative litigation may have been influenced by the SEC case. Benjamin P. Edwards, *Cybersecurity Oversight Liability*, 35 GA. STATE UNIV. L. REV. 663, 675 (2019).

184. Altaba Inc., *supra* note 182, at *8.

185. Pearson plc, Securities Act Release No. 10,963, Exchange Act Release No. 92,676, 2021 WL 3627064 (Aug. 16, 2021).

186. NAT'L ASS'N OF CORP. DIRS. ET AL., *supra* note 58, at 6.

187. Press Release, SEC, SEC Announces Three Actions Charging Deficient Cybersecurity Procedures (Aug. 30, 2021), https://www.sec.gov/news/press-release/2021-169 [https://perma.cc/LY3C-NKP2].

188. Press Release, SEC, SEC Charges Issuer with Cybersecurity Disclosure Controls Failures (June 15, 2021), https://www.sec.gov/news/press-release/2021-102 [https://perma.cc/HW48-UXF5].

189. S. 808, 117th Cong. (2021); 167 CONG. REC. S1617 (daily ed. Mar. 17, 2021) (statement of Sen. Jack Reed). Reed (D-R.I.) introduced the bill on behalf of Sen. Susan Collins (R-Me.), Sen. Mark Warner (D-Va.), Sen. Kevin Cramer (R-N.D.), Sen. Catherine Cortez Masto (D-Nev.), and Sen. Ron Wyden (D-Or.). *Id.*

cyber related attacks."[190] Though the CDA remains just a proposal, almost exactly one year after its introduction, on March 9, 2022, the SEC proposed new cybersecurity rules that included an explicit focus on the cybersecurity oversight role of corporate boards.[191]

The SEC pointed to several factors motivating the 2022 rule proposal: (1) the Commission's observation that "certain cybersecurity incidents that were reported in the media . . . were not disclosed in a registrant's filings;" (2) inconsistent specificity in disclosures; and (3) inclusion of the cybersecurity content "with other unrelated disclosures, which makes it more difficult for investors to locate, interpret, and analyze the information provided."[192]

In July 2023, the SEC released the finalized Cybersecurity Rules.[193] Under these new Rules, companies must disclose specifics about their cybersecurity risks and strategies, including risks created by third-party services,[194] management positions with a responsibility for cybersecurity risk assessment and the expertise of such individuals,[195] and use of external services to manage cybersecurity risk.[196] Additionally, the Rules specify the information companies must disclose about the material impact of attacks or threats that have risen to a material level.[197] Though the scope of this disclosure was narrowed somewhat, based on concerns voiced in the comments,[198] the finalized Rules did adopt the proposed requirement to disclose a material cybersecurity incident within four days of its discovery.[199]

Like the CDA, the SEC's Cybersecurity Rules reflect an increasing focus "on the role of boards in preventing, mitigating, and, where necessary, disclosing cybersecurity

190. 167 Cong. Rec. S1617 (daily ed. Mar. 17, 2021) (statement of Jack Reed).

191. *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Securities Act Release No. 11,038, Exchange Act Release No. 94,382, Investment Company Act Release No. 34,529, 87 Fed. Reg. 16590, 16593 (proposed March 9, 2022) (to be codified at 17 C.F.R. §§ 229, 232, 239, 240, 249) [hereinafter SEC 2022 Proposed Rules]; Press Release, SEC, SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, (March 9, 2022) [hereinafter Proposed Rule Press Release], https://www.sec.gov/news/press-release/2022-39 [https://perma.cc/G2EB-JAV2].

192. SEC 2022 Proposed Rules, *supra* note 191, at 16594; *see also* Gary Gensler, SEC Chair, Statement on Public Company Cybersecurity Disclosures (July 26, 2023), https://www.sec.gov/news/statement/gensler-statement-cybersecurity-072623 [https://perma.cc/UJX2-XQ64] ("[S]taff have observed that [previously issued guidance] has not resulted in sufficiently consistent, comparable, and decision useful disclosures.").

193. SEC 2023 Cybersecurity Rules, *supra* note 18.

194. *See id.* at 51904, 51910.

195. *Id.* at 51914–15.

196. *Id.* at 51913.

197. *See id.* at 51899 ("Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its: —Nature, scope, and timing; and —Impact or reasonably likely impact.").

198. *Id.* at 51903 ("First, we are narrowing the amount of information required to be disclosed . . . . And second, we are providing for a delay for disclosures that would pose a substantial risk to national security or public safety . . . ."); *id.* at 51904 ("We are not adopting, as proposed, a requirement for disclosure regarding the incident's remediation status, whether it is ongoing, and whether data were compromised.").

199. *Id.* at 51899.

incidents."[200] Though the finalized Rules regarding board oversight are "less granular than proposed"[201] they still aim to allow investors to see how a company's board oversees its cybersecurity processes.[202] The Rules specify that "registrants must '[d]escribe the board's oversight of risks from cybersecurity threats,' and . . . 'identify any board committee . . . responsible' for such oversight 'and describe the processes by which the board . . . is informed about [cybersecurity] risks.'"[203]

Though the rules became effective in December 2023, an October 2023 enforcement action perhaps previews what companies should anticipate from SEC enforcement of the Cybersecurity Rules. The SEC brought charges against SolarWinds Corporation, and its chief information security officer, "for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities."[204] In 2020, SolarWinds was the target of a massive cyberattack that had significant and widespread impacts on private and government organizations across the United States.[205] The SEC complaint alleged that the company publicly overstated its cybersecurity practices and "misled investors by disclosing only generic and hypothetical risks at a time when the company and [its chief information security officer] knew of specific deficiencies in SolarWinds' cybersecurity practices as well as the increasingly elevated risks the company faced at the same time."[206]

III. DISCUSSION

The Discussion considers the SEC's Cybersecurity Rules in light of the shortcomings of the prior discretionary approach to disclosure and concludes that the Rules both create the potential to provide investors with a more complete risk picture and present significant implementation challenges for regulated companies. Part A

200. NAT'L ASS'N OF CORP. DIRS. ET AL., *supra* note 58, at 10; *see, e.g.*, Luis Aguilar, SEC Comm'r, Speech at the New York Stock Exchange Cyber Risks and the Boardroom Conference: Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (June 10, 2014), https://www.sec.gov/news/speech/2014-spch061014laa [https://perma.cc/DR55-TQC3]; COUNCIL OF INST. INVS., PRIORITIZING CYBERSECURITY: FIVE INVESTOR QUESTIONS FOR PORTFOLIO COMPANY BOARDS 2 (2016) [hereinafter CII, PRIORITIZING CYBERSECURITY], https://www.cii.org/files/publications/misc/4-27-16%20 Prioritizing%20Cybersecurity.pdf.

201. SEC 2023 Cybersecurity Rules, *supra* note 18, at 51914.

202. *Id.* at 51896 (highlighting the aim of the rules to "enhance and standardize" disclosures in areas including governance and board oversight of cybersecurity risks).

203. *Id.* at 51914.

204. Press Release, SEC, SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures (Oct. 30, 2023) [hereinafter SolarWinds Press Release], https://www.sec.gov/ news/press-release/2023-227 [https://perma.cc/723Q-ZRFJ]; *see also* Complaint & Demand for Jury Trial at 1–2, SEC v. SolarWinds Corp., No. 23-CIV-9518 (S.D.N.Y. Oct. 30, 2023) ("SolarWinds' public statements about its cybersecurity practices and risks painted a starkly different picture from internal discussions and assessments about the Company's cybersecurity policy violations, vulnerabilities, and cyberattacks.").

205. Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack*, NPR (April 16, 2021, 10:05 AM), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack [https://perma.cc/9523-UMHB] ("Hackers believed to be directed by the Russian intelligence service, the SVR, used that routine software update to slip malicious code into Orion's software and then used it as a vehicle for a massive cyberattack against America.").

206. SolarWinds Press Release, *supra* note 204.

addresses the failures of the discretionary approach. Part B considers the potential positive outcomes for investors. Part C examines the implications of mandatory disclosures for board oversight. Finally, Part D highlights two significant unresolved issues—the materiality standard and the risks inherent in disclosing details of a cyberattack while it remains ongoing.

A. The Problem with Discretionary Cybersecurity Disclosures

The SEC's cybersecurity disclosure guidance prior to 2023 failed to elicit robust and consistent reporting across regulated companies.[207] Under the guidance, companies did not always disclose events transparently, and disclosures lacked specificity.[208] Additionally, the inconsistencies in the location of cybersecurity information on the various forms made it difficult for investors to easily locate the information and compare disclosures across companies.[209]

As one scholar notes, without uniform requirements, "management can be expected to approach risk-related disclosures conservatively because disclosure is costly and may benefit competitors."[210] And when companies fail to identify and quantify new risks, investors cannot assess their magnitude.[211] Where there is a lack of transparency, there is an information asymmetry—cyber criminals "know more about the information security practices of entities than most of the entities' shareholders."[212] A discretionary system also results in a lack of uniformity that impedes comparability of information.[213] These disclosure shortcomings arguably create an externality for investors, exposing them to risk they are not compensated for bearing.[214]

B. The Investor Perspective

For investors, there is an obvious business case for companies to address the risk of cyberattacks, as they have the potential to paralyze business operations, expose the company to legal and regulatory costs, destroy company value, and damage shareholder earnings.[215] In 2020, the director of the federal government's Cybersecurity and Infrastructure Security Agency (CISA) stated that cybersecurity

---

207. *See* Ferrillo et al., *supra* note 118.

208. See *supra* note 192 and accompanying text regarding the SEC discussion of factors motivating the 2022 Proposed Rules.

209. See *supra* note 192 and accompanying text discussing motivating concerns.

210. Harper Ho, *Risk-Related Activism*, *supra* note 82, at 669.

211. *Id.* at 657.

212. Matawyshn, *supra* note 50, at 194.

213. Fisch, *supra* note 161, at 926–27, 947; *see also* Stewart, *supra* note 108, at 3 ("In the absence of the more specific requirements in the [2022] Proposal, many companies likely will continue to provide inadequate information on their processes, responses and level of vulnerability, as noted in the Proposal.").

214. Harper Ho, *Risk-Related Activism*, *supra* note 82, at 669; *see also* Bambauer, *supra* note 64, at 1077 ("[I]nsecurity creates a negative externality. Insecure organizations pass costs to others, even if only in the form of risk, without being penalized for them."); Stewart, *supra* note 108, at 3 ("The lack of timely, comprehensive disclosure of material cyber events exposes investors and the community at large to potential harm.").

215. PRINCIPLES FOR RESPONSIBLE INV., *supra* note 14, at 4.

incidents "can no longer be looked at as a mere IT problem. Rather, these incidents represent potential business losses (either realized or unrealized) that must be treated with the same vigilance as more traditional vectors of business disruption and loss of profit."[216] Investor groups have called for stronger cyber-risk management practices by boards.[217] In 2016, for example, the Council of Institutional Investors, a group representing corporate and other investor entities with combined assets under management of approximately $4 trillion,[218] stated that "[e]ffective cybersecurity risk management starts with the board."[219]

The 2023 Cybersecurity Rules have the potential to benefit investors and markets. First, by moving to mandatory disclosures and increasing the specificity required, the Rules have the potential to increase the "consistency, completeness and comparability of information across registrants."[220] Individual shareholders will have additional information that can be used to align their investment decisions with prospects of future cash flow and with their own risk appetite.[221] Additionallly, when all companies are compelled to uniformly and regularly disclose detailed cybersecurity risk information, "investors [will be able to] more readily identify outliers and pressure a change in their policies."[222]

At the market level, the increased transparency requirements of the Rules are intended to ensure "that corporate information vulnerability, security losses, and diminution of intangible asset value are being correctly factored into the stock price of

---

216. Kolasky, *supra* note 92, at 4; *see also* Neuberger, *supra* note 4, at 1 ("The most important takeaway from the recent spate of ransomware attacks . . . is that companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively.").

217. *See* CII, PRIORITIZING CYBERSECURITY, *supra* note 200, at 1 ("[I]nvestors are looking to boards for leadership in addressing the risks and mitigating the damage associated with cyber incidents. Cybersecurity is an integral component of a board's role in risk oversight."); PRINCIPLES FOR RESPONSIBLE INV., *supra* note 14, at 9 ("Investors increasingly expect cyber security issues to fall within the remit of company boards and their sub-committees given the potential physical and economic implications of a cyber security incident on business operations."); CII, GOVERNANCE POLICIES, *supra* note 106, § 2.7, at 7.

218. Council of Institutional Investors is "a nonprofit, nonpartisan association of U.S. public, corporate and union employee benefit funds, other employee benefit plans, state and local entities charged with investing public assets, and foundations and endowments with combined assets under management of approximately $4 trillion." *About CII*, COUNCIL OF INST. INVS., https://www.cii.org/about (last visited Nov. 22, 2023).

219. CII, PRIORITIZING CYBERSECURITY, *supra* note 200, at 2.

220. SEC, REPORT ON REVIEW OF DISCLOSURE REQUIREMENTS OF REGULATION S-K 98 (2013), https://www.sec.gov/news/studies/2013/reg-sk-disclosure-requirements-review.pdf [https://perma.cc/KS2X-W9VP]; *see also* SEC 2023 Cybersecurity Rules, *supra* note 18, at 6–7 (noting that "companies provide different levels of specificity regarding the cause, scope, impact, and materiality of cybersecurity incidents" and that cybersecurity risk disclosures on annual 10-K reports "are sometimes included with other unrelated disclosures, which makes it more difficult for investors to locate, interpret, and analyze the information provided").

221. *See* Matawyshn, *supra* note 50, at 194; Berkman et al., *supra* note 110, at 522 ("[E]xpanding the measure of cybersecurity awareness . . . can help investors and other market participants to incorporate cyber awareness in their decision-making.").

222. Fisch, *supra* note 161, at 948.

vulnerable entities."[223] This, in turn, may serve to further insulate investors from financial losses by minimizing stock price volatility.

C. Focus on Board Oversight

By requiring companies to regularly disclose details of their cybersecurity strategy and report cyber-events, the Cybersecurity Rules may encourage boards to engage more frequently and fully with cybersecurity oversight.[224] In particular, the requirement to disclose cybersecurity procedures and policies may lead boards to adjust their oversight of management by, for example, asking more informed questions, critically evaluating management strategies, and verifying that they have effective internal controls in place.[225] Mandatory disclosure may also reframe the board's decision to invest in cybersecurity, "changing good security from a luxury to an essential business expense that must be incurred by all entities."[226] Because the Rules require detailed disclosures related to risk-assessment programs, boards may be incentivized, for example, to take the costly step of instituting continuous threat monitoring.[227]

Insofar as the Rules encourage effective board oversight of cybersecurity, they have the potential to decrease investor vulnerability by reducing the exposure of companies to cyberattacks and, in turn, the associated stock price drops and other short- and long-term financial harms.[228] There is evidence that companies without board oversight of risk management experience a stock price reaction to a cyberattack that is four percentage points lower than those with board oversight of risk management.[229] Conversely, a 2018 study found that an increase in a company's cybersecurity awareness was associated with a $2.30 stock price increase.[230]

D. Unresolved Issues

Though the SEC's 2023 Cybersecurity Rules promise benefits for investors and companies, important questions remain. Two stand out as particularly difficult to resolve and will likely be the focus of significant debate as registrants begin complying

223. Matawyshn, *supra* note 50, at 136.

224. Fisch, *supra* note 161, at 951 ("[A]n additional value to an affirmative disclosure requirement is its ability to focus board and management attention on acquiring information and exercising oversight.").

225. *See* Berkman et al., *supra* note 110, at 512 ("Firms with better cybersecurity awareness are thus in a better position to prevent a cyber incident from occurring or to minimize the cost of a cyber incident.").

226. Matawyshn, *supra* note 50, at 193; *see also* Stewart, *supra* note 108, at 2 ("We believe the disclosed information will . . . provide incentives for companies to implement effective cybersecurity strategies.").

227. The Rules require companies to disclose whether they "engage[] assessors, consultants, auditors, or other third parties in connection with [risk management] processes." SEC 2023 Cybersecurity Rules, *supra* note 18, at 63.

228. See *supra* Part II.B discussing harms resulting from cyberattacks.

229. Kamiya et al., *supra* note 8, at 733.

230. Berkman et al., *supra* note 110, at 509, 522 (citing a 2018 study that found "a positive association between [a corporation's] cybersecurity awareness and market value").

with the requirements. First, the materiality standard is unclear and evolving.[231] Materiality cannot be analyzed with a bright-line test and "depends not upon the literal truth of statements, but upon the ability of reasonable investors to become accurately informed."[232] Commentators note the "amorphous character" of the standard,[233] and one goes so far as to assert that it has been "a hopeless morass of disparate caselaw for decades."[234]

Beyond general problems with materiality, the standard has not yet been clarified with regard to cybersecurity disclosures.[235] Because materiality is contextual, cyber-incident harm thresholds for established and emerging growth companies may vary widely.[236] Enforcement actions provide some indication of the SEC's interpretation of the cybersecurity materiality standard, but SEC guidance is still needed to clarify the standard for the full range of regulated companies.

A second significant issue is the difficulty a company faces when trying to balance disclosure compliance against the risk of increasing its own vulnerability or giving an advantage to market competitors.[237] These competing interests are particularly problematic in the context of the proposed requirement to disclose an incident within four days of discovery.[238] Despite the potential value of this information to investors, disclosing details about an unresolved attack could foreseeably increase a company's vulnerability.[239] As one scholar observes, "Long-term investors would likely prefer that the firm avoid any disclosures that increase the firm's exposure to losses, even if that means a less accurate price for its stock in the short term because some risks or threats remain hidden from the public."[240] Boards will have to carefully consider and balance disclosure rules and risks.

IV. CONCLUSION

The SEC's 2023 Cybersecurity Rules promise substantial benefits for corporate governance, shareholder risk management, and market accuracy. By directing the attention of corporate boards to cybersecurity oversight, they may also serve to harden American targets against increasingly sophisticated large-scale cyberthreats. The full

231. *See* Fisch, *supra* note 161, at 936–37 (noting the "unclear" and "evolving" scope of the SEC's materiality definition and discussing the Commission's position shifts with regard to the materiality of sustainability information).

232. Morse et al., *Cybersecurity Guidelines*, *supra* note 80, at 4 (quoting HAZEN, *supra* note 168, § 3.10).

233. *Id.*

234. Matawyshn, *supra* note 50, at 186.

235. Morse et al., *Cybersecurity Guidelines*, *supra* note 80, at 9–11.

236. *See id.* at 11 ("The magnitude of these expenditures or expected future effects may not be expected to reach materiality thresholds in many firms.").

237. WOLFF, *supra* note 31, at 263 ("No company wants to be the first to release that data about the threats they see and the impact of their countermeasures, for fear of drawing attention to their security incidents. Furthermore, no company stands to gain anything by unilaterally releasing such information . . . .").

238. *See* Morse et al., *Cybersecurity Guidelines*, *supra* note 80, at 15; WOLFF, *supra* note 31, at 262.

239. Morse et al., *Cybersecurity Guidelines*, *supra* note 80, at 15.

240. *Id.* at 16.

implications of the Rules are yet uncertain, though, given the lack of clarity regarding the application of the materiality standard and the significant unknowns surrounding the incident disclosure requirements.