WEIGHING THE POTENTIAL HARM OF THE SEC'S PROPOSED CYBERSECURITY INCIDENT REPORTING RULES

AUTHOR: J. CURTIS HAUSCHILDT

I. Introduction

The threat posed by malicious cyber activity affects virtually every industry. Yet, despite this danger – whether through cyber-enabled extortion, theft, or other forms of attack – many sectors have only recently begun making a concerted effort to prevent it. In some industries, it has fallen to regulatory agencies to ensure that proper care has been taken to protect stakeholders. This is as true for the financial sector as any other.

However, when an agency sets out to craft a regulatory regime in a field foreign to its standard area of expertise, it can, despite its best intentions, do more harm than good. The Securities and Exchange Commission (SEC) may have done so with three of its proposed rules designed to increase cybersecurity. While the proposed rules largely appear to achieve their goal to prevent cybersecurity incidents and inform stakeholders of cybersecurity-related risks, each contains a mandatory reporting regime requiring immediate, public reporting of cybersecurity incidents that poses a real danger to the interests of corporations, shareholders, and national security.

This paper examines whether the SEC's proposed rules on cybersecurity are likely to accomplish its stated objective of providing a benefit to the financial industry and its stakeholders through a speedy, partially public-facing cybersecurity incident reporting regime. First, it investigates three of the SEC's proposed rules, examines their stated purposes, and compares their most relevant elements. Next, it raises potential threats the proposed rules could pose to various stakeholders if adopted in their current form – focusing on the immediacy, publicity, and interconnectedness of their reporting requirements. Finally, it examines potential solutions to mitigate these risks and considers their effect on the financial regulatory industry.

II. The SEC's Proposed Cybersecurity Rules

The SEC has put forward a large and ambitious regulatory agenda since Chairman Gary Gensler assumed office in early 2021, attempting to usher in sweeping updates in several key areas.[1] One recent focus has been cybersecurity. Three of the SEC's recently proposed rules, in particular, promise to have an outsized effect if they are adopted in their current forms. They are: (1) Cybersecurity Risk Management Rules and Amendments for Investment Advisers, Registered Investment Companies, and Business Development Companies (Proposed Rule for Investment Advisors and Funds);[2] (2) Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (Proposed Rule for Public Companies);[3] and (3) Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents (Proposed Rule for Market Entities).[4] All three proposed rules target different groups within the securities industry and have nuanced differences to reflect this, but their substance can be divided into three broad categories: immediate reporting on significant

---

1 *See generally* U.S. SEC. AND EXCH. COMM'N., THE INSPECTOR GENERAL'S STATEMENT ON THE SEC'S MANAGEMENT AND PERFORMANCE CHALLENGES, 2 (Oct. 13, 2022) ("in only the first 8 months of 2022, the SEC proposed 26 new rules...more than twice as many new rules as proposed the preceding year and more than it had proposed in each of the previous 5 years"); Bob Pisani, *SEC Chairman Gary Gensler Embarks on Ambitious Regulatory Agenda. What it Means for Investors*, CNBC (Feb. 04, 2022), https://www.cnbc.com/2022/02/04/sec-chair-gary-gensler-embarks-on-ambitious-regulatory-agenda-what-it-means-for-investors.html ("This is one of the largest regulatory agendas we have seen from the SEC in many years.").

2 Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13,524 (proposed Feb. 09, 2022) (to be codified at 17 C.F.R. pts. 230, 232, 239, 270, 274, 275, and 279) [hereinafter Proposed Rule for Investment Advisors and Funds].

3 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 20,212 (proposed Mar. 09, 2022) (to be codified at 17 C.F.R. pts. 229, 232, 239, 240, and 249) [hereinafter Proposed Rule for Public Companies].

4 Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, 87 Fed. Reg. 16,590 (proposed Mar. 15, 2023) (to be codified at 17 C.F.R. pts. 232, 240, 242, and 249) [hereinafter Proposed Rule for Market Entities].

cybersecurity incidents; periodic reporting on all cybersecurity incidents; and increased disclosure of companies' risk management, strategy, governance, and recordkeeping regarding cybersecurity risks.

This paper will focus predominantly on the first category, as it poses a potential threat to national security and stakeholder interests due to the unique effects timeliness and publicity have on cybersecurity incident reporting. The requirements found in the second and third categories appear comparable to the levels of useful disclosure found in non-cybersecurity reporting requirements and, although they will surely have an impact on the entities being regulated, will not be thoroughly investigated in this paper.

A. Why the SEC is Concerned with Cybersecurity

The SEC is rightly concerned about the danger posed by cyber attacks. The cyber-capabilities of malicious actors continues to grow in sophistication and new cyber-actors continue to emerge.[5] Concurrently, the attack surface presented by the U.S. government and U.S. businesses continues to expand, and growing digital interconnectedness presents an increasing likelihood of wider spread and greater impact resulting from any individual cyber attack.

In 2021, $10.3 billion was reported lost due to cybercrime to the U.S. Federal Bureau of Investigations.[6] This figure represents a steady rise over the past five years and does not factor in unreported theft, which would likely make the true figure much higher. Although the SEC specifically cites cyber criminals and their growing sophistication, state actors remain a threat, as well. North Korea has "conducted cyber theft against

[5] OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY, 16 (Apr. 09, 2021).

[6] U.S. FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2022, 7 (Mar. 2023).

financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars"[7] and Iran has been responsible for "cyber crimes that cost U.S. financial institutions tens of millions of dollars."[8] Even more threatening would be a concentrated attack by a more capable state threat, such as China or Russia, in an attempt to destabilize the U.S. financial system.[9]

The United States is also likely to be a much better target than in the past. The combination of a vast rise in the volumes of electronically stored data, the digitalization of almost all modern day business, a reliance on third party digital services, and the increase in remote work have all severely increased the amount of attack surface available to potential malicious actors.[10] Additionally, the world's growing interconnectedness increases the likelihood of systemic attacks or cyber spillover, especially within sectors.[11] These two factors greatly raise the probability of a cyber attack successfully occurring and then spreading widely, causing significant follow-on effects to the businesses affected, their investors, and national security.

B. Proposed Rule for Investment Advisers and Funds

On February 09, 2022, the SEC proposed a set of rules and related amendments "designed to address cybersecurity risks that could harm advisory clients and fund investors."[12] The SEC received a number of comments regarding the proposed rule – including from notable U.S. senators, investment advisers, and financial associations -

---

7 OFF. OF THE DIR. OF NAT'L INTEL., *supra* note 5.

8 *Iranians Charged with Hacking U.S. Financial Sector*, U.S. FED. BUREAU OF INVESTIGATION (Mar. 24, 2016), https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector#.

9 *See generally* Proposed Rule for Market Entities, *supra* note 4, at 20232 ("threat actors could seek to disrupt their functions for geopolitical purposes").

10 Proposed Rule for Public Companies, *supra* note 3, at 16591.

11 Proposed Rule for Public Companies, *supra* note 3, at 16592.

12 U.S. SEC. AND EXCH. COMM'N., *Cybersecurity Risk Management*, Fact Sheet (Feb. 09, 2022), https://www.sec.gov/files/33-11028-fact-sheet.pdf.

before the comment period was reopened for an additional 60 day period on March 15, 2023.[13] This was done partly to allow commentators to consider the effects of several new cybersecurity proposals[14] on the proposed rule but also allowed additional commentary on one of the most contentious features of the proposed rule – mandatory reporting of "significant cybersecurity incidents" within forty-eight hours.[15]

The requirement mandates that covered actors report any significant cybersecurity incidents to the SEC through a Form ADV-C within forty-eight hours of becoming aware of it, regardless of whether it has ceased or is still occurring.[16] The Form ADV-C would include both general and specific questions regarding the cybersecurity incident, including the nature of the incident, its severity, and whether any disclosure has been made to clients or investors.[17] The proposed rule also requires that updates are made to the Form ADV-C within forty-eight hours if any of the previously reported information becomes materially inaccurate or new material information about the reported cybersecurity incident is discovered, and it must be amended after the cybersecurity incident is resolved or upon closing a related internal investigation.[18]

---

13 *Comments on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, U.S. SEC. AND EXCH. COMM'N., https://www.sec.gov/comments/s7-04-22/s70422.htm (last visited May 14, 2023).

14 These include the Proposed Rule for Market Entities, as well as the Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information Release and the Regulation Systems Compliance and Integrity Release. The latter two are not explicitly relevant to this paper's topic and are thus not explored in detail. *Reopening of Comment Period for "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies"*, U.S. SEC. AND EXCH. COMM'N. (Mar. 15, 2023), https://www.sec.gov/rules/proposed/2023/33-11167.pdf.

15 U.S. SEC. AND EXCH. COMM'N., *SEC Reopens Comment Period for Proposed Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds*, Press Release (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-54; Paul Mulholland, *SEC Reopens Comment Period on Cybersecurity Rule*, CHIEF INV. OFFICER (Mar. 21, 2023).

16 Proposed Rule for Investment Advisers and Funds, *supra* note 2, at 13536.

17 Proposed Rule for Investment Advisers and Funds, *supra* note 2, at 13536.

18 Proposed Rule for Investment Advisers and Funds, *supra* note 2, at 13536.

The triggering event for reporting is not a definitive conclusion that a significant cybersecurity incident has occurred but merely a "reasonable basis to conclude that an incident has occurred or is occurring."[19] A cybersecurity incident is considered "significant" if it (1) significantly disrupts or degrades an adviser's[20] or fund's ability to maintain critical operations or (2) leads to the unauthorized access or use of adviser or fund information, which results in substantial harm to the adviser or fund, or to a client or investor whose information was accessed.[21]

Notably, discretion for whether the Form ADV-C is disclosed to the public lies with the SEC, which is required to publicly disclose such information unless a disclosure is found to be "neither necessary nor appropriate in the public interest or for the protection of investors."[22] This would seemingly make disclosure of a significant cybersecurity incident – within forty-eight hours of its discovery, regardless of whether it is ongoing – the default position. Although the Commission has stated its preliminary view is that any Form ADV-C regarding a cybersecurity incident should be confidential, this is merely an initial decision.[23] Such a decision could be reversed before a final rule is released or at any time afterwards, providing no concrete privacy protection.

C. Proposed Rule for Public Companies

On March 09, 2022, the SEC announced a set of proposed rules and related amendments designed to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting" by public

---

19 Proposed Rule for Investment Advisers and Funds, *supra* note 2, at 13537.

20 Or the ability of the adviser's clients.

21 Proposed Rule for Investment Advisers and Funds, *supra* note 2, at 13536-37.

22 Proposed Rule for Investment Advisers and Funds, *supra* note 2, at 13539 (citing Investment Advisers Act of 1940, 15 U.S.C. § 80b-10(a)).

23 *See* Proposed Rule for Investment Advisers and Funds, *supra* note 2, at 13539.

companies.[24] The SEC received approximately 150 comments regarding the proposed rule – including comments from notable U.S. senators, cybersecurity experts, law firms, and corporate associations - before the comment period ended.[25]

The proposed rule would require registrants to report material cybersecurity incidents[26] in a modified Form 8-K within four business days of discovery of a material cybersecurity incident.[27] This requires the registrant to both identify that a cybersecurity incident has occurred and that the incident was material to investors. In order to prevent the registrant from delaying such a determination, the registrant is required to "make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."[28] Reporting requirements would not be delayed for ongoing internal or external investigations of a cybersecurity incident.[29]

The information required to be filed within the modified Form 8-K includes the nature and scope of the incident, when the incident was discovered, whether it is ongoing, whether any data was accessed or stolen, the effect of the incident on the registrant's operations, and whether a response plan had been initiated.[30] The disclosures made in the modified Form 8-K would be public, just as with current Form 8-K submissions.[31]

---

[24] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16,590 (proposed Mar. 09, 2022) (to be codified at 17 C.F.R. pts. 229, 232, 239, 240, and 249); U.S. SEC. AND EXCH. COMM'N., *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*, Press Release (Mar. 09, 2022), https://www.sec.gov/news/press-release/2022-39.

[25] *Comments on the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, U.S. SEC. AND EXCH. COMM'N., https://www.sec.gov/comments/s7-09-22/s70922.htm (last visited May 14, 2023).

[26] What constitutes materiality in this setting is consistent with what a corporation would consider in any other setting, namely whether "'there is a substantial likelihood that a reasonable shareholder would consider it important'...or if it would have 'significantly altered the `total mix' of information made available.'" Proposed Rule for Public Companies, *supra* note 3, at 16596 (quoting *TSC Indus.* v. *Northway,* 426 U.S. 438, 449 (1976)).

[27] Proposed Rule for Public Companies, *supra* note 3, at 16595.

[28] Proposed Rule for Public Companies, *supra* note 3, at 16595-96.

[29] Proposed Rule for Public Companies, *supra* note 3, at 16596.

[30] Proposed Rule for Public Companies, *supra* note 3, at 16595.

[31] *See* Proposed Rule for Public Companies, *supra* note 3, at 16595.

D. Proposed Rule for Market Entities

On March 15, 2023, the SEC proposed a new rule, form, and related amendments designed to address the cybersecurity risks of "Market Entities," a term that includes "broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents."[32] The proposed rule would require Market Entities to immediately provide the SEC with written notification when they have a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring.[33] The Market Entity must also file Part I of proposed Form SCIR within forty-eight hours of that time.[34] Depending on the type of Market Entity, a written report and Part I of proposed Form SCIR must be filed with other supervisory authorities, as well.[35]

The information to be provided in Part I of proposed Form SCIR would include the nature and scope of the cybersecurity incident, its effect on critical systems, whether the threat actor conducting the incident had been identified, whether data or assets had been accessed or stolen, and whether a response plan had been initiated.[36] Much like the Proposed Rule for Investment Advisers and Funds, the proposed Form SCIR must be amended within forty-eight hours if any of the previously reported information becomes materially inaccurate or new material information about the reported cyber incident is discovered, and it must be amended after the cyber incident is resolved or upon closing a

---

32 U.S. SEC. AND EXCH. COMM'N., *SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets*, Press Release (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-52.

33 Proposed Rule for Market Entities, *supra* note 4, at 20248.

34 Proposed Rule for Market Entities, *supra* note 4, at 20249.

35 Proposed Rule for Market Entities, *supra* note 4, at 20249.

36 Proposed Rule for Market Entities, *supra* note 4, at 20251-54.

related internal investigation.[37] The definition of a significant cybersecurity incident is relatively indistinguishable to that used in the Proposed Rule for Investment Advisers and Funds, substituting Market Entities for investment advisers and funds.[38]

Both the immediate written notice and Part I of proposed Form SCIR are designed to be confidential and would not be made public to the extent permitted by law.[39] However, summary descriptions of all significant cybersecurity incidents experienced during the current and previous calendar years would need to be publicly reported in Part II of proposed Form SCIR, which must be filed with the SEC and posted on an "easily accessible" portion of the Market Entity's website annually and when updated.[40] It would also need to be provided to customers when they open accounts.[41]

Because an updated Part II is required to be filed and posted "promptly...after the occurrence of a new significant cybersecurity incident" the privacy intent behind Part I's confidentiality is significantly diminished.[42] A Market Entity would be required to immediately and publicly disclose that a significant cybersecurity incident has occurred, even if it is still ongoing.

---

37 Proposed Rule for Market Entities, *supra* note 4, at 20249-50.

38 *See* Proposed Rule for Market Entities, *supra* note 4, at 20233 (defining a significant cybersecurity incident as cybersecurity incident, or a group of related incidents, that (1) significantly disrupts or degrades the ability of a Market Entity to maintain critical operations or (2) leads to the unauthorized access or use of the Market Entity's information or information systems, which results in or is reasonably likely to result in substantial harm to the Market Entity or a customer, counterparty, member, registrant, or user of the Market Entity, or to any other person that interacts with the Market Entity).

39 Proposed Rule for Market Entities, *supra* note 4, at 20249.

40 Proposed Rule for Market Entities, *supra* note 4, at 20257.

41 Proposed Rule for Market Entities, *supra* note 4, at 20257.

42 *See* Proposed Rule for Market Entities, *supra* note 4, at 20257-58.

III. Potential Dangers of the Proposed Rules

A high volume of concern about the proposed rules' cybersecurity incident reporting requirements – and the dangers they may pose to the financial industry, stakeholders, and national security – has been raised during the commenting period, in direct discourse with the SEC, and even from within the SEC itself. The biggest potential pitfalls include the tight time windows required for mandatory reporting, the public nature of the reporting, and how these requirements would interact with each other and the complicated web of cybersecurity incident reporting requirements already present at the national and state levels. All of these factors also lead to the overarching question of whether the SEC is the actor best suited to respond to the reported cybersecurity incidents and, if not, what is the benefit of these SEC-mandated reports?

A. Dangers Posed by Immediate Reporting

A short mandatory reporting period provides several challenges to the recipient of a cyber attack, primarily in taking attention and resources away from stopping the event. In many cases, the team responsible for identifying and resolving the issues would also be the ones responsible for producing a report. Competing priorities could negatively impact the efficacy of the cybersecurity mitigation response and result in sparse or potentially incorrect reporting as neither job received full attention.[43] The SEC requirements may serve to "distract employees...from mitigating the immediate threat to the firm and its customers as they navigate the aggressive deadlines and open-ended information

[43] Patrick Donachie, *Is 48 Hours Too Short for Reporting Cybersecurity Breaches?*, WEALTHMANAGEMENT (Mar. 14, 2023), https://www.wealthmanagement.com/regulation-compliance/48-hours-too-short-reporting-cybersecurity-breaches#menu (reporting concerns raised at the IAA's 2023 Investment Adviser Compliance Conference); Mulholland, *supra* note 15 ("cybersecurity employees...who are responsible for fixing and mitigating the breach will also be responsible for reporting. This means the reporting requirement essentially becomes a burden and a distraction while an incident is ongoing").

demands."[44] The requirement to continually update the SEC on the situation means this potential distraction would continue until the cybersecurity incident had ended.

While the four days required by the Proposed Rule for Public Companies may be enough to provide a relatively accurate report, depending heavily on the nature and scope of the cyber incident, the reporting windows of the other two proposed rules – ranging from "immediate" to forty-eight hour – is almost certainly too short of a time to respond with any meaningful information regarding a significant cybersecurity incident.[45]

B. Dangers Posed by Public Reporting

Although the three proposed rules all recognize the harm that public disclosure may have, their requirements do not provide meaningful protection. Despite noting that "public disclosure may harm an adviser's or fund's ability to mitigate or remediate the cybersecurity incident, especially if the incident is ongoing"[46] and that certain levels of disclosure may "reveal information...that could be used by threat actors to cause harm,"[47] the public reporting posture actually adopted in the proposed rules poses a threat to the reporting company, to national security, and to investors and shareholders.

Releasing information regarding a cybersecurity incident before the vulnerability has been fixed makes it significantly harder to catch the malicious actor and can highlight weaknesses in a company's defenses to other bad actors. All three proposed rules increase these risks. The disclosures made in the Proposed Rule for Public Companies would be

---

44 Commissioner Hester M. Peirce, U.S. SEC. AND EXCH. COMM'N., *Statement on Proposed Cybersecurity Rule 10 and Form SCIR*, Statement (Mar. 15, 2023), https://www.sec.gov/news/statement/peirce-statement-enhanced-cybersecurity-031523.

45 *See id.*; Ari Schwartz, *The SEC Obstructs National Security*, WALL ST. J. (Sep. 29, 2022), https://www.wsj.com/articles/the-sec-obstructs-national-security-cyber-attack-defense-corporations-cybersecurity-china-india-public-disclosure-report-11664487542.

46 Proposed Rule for Investment Advisers and Funds, *supra* note 2, at 13539

47 Proposed Rule for Market Entities, *supra* note 4, at 20256.

made public four days after their discovery and the Proposed Rule for Market Entities would require a summary of any significant cybersecurity incident to be made public within forty-eight hours.[48] Although the SEC has stated a preliminary view that disclosure of cybersecurity incidents should be kept private in the Proposed Rule for Investment Advisers and Funds, this is inadequate protection as the initial policy decision could be reversed before the final rule is issued or any time afterwards. Such a change would make all reports public. This early publicity poses significant potential danger.

It is rare for a serious cybersecurity incident to be resolved within four days of its discovery, and it is nearly impossible to do so within forty-eight hours.[49] Premature disclosure of vulnerability-related information is "inconsistent with industry best practices for security and...further undermin[es] the security posture of impacted parties, and the security of the nation and society more broadly."[50] Announcing a successful attack, even just in summary form, puts a company at a much higher risk of successive attacks from additional malicious cyber actors by alerting the public of vulnerabilities.[51] Even just notification, without any details or summary, is enough to do serious damage. Notifying the attacker of such discovery while the investigation is ongoing makes it much more likely that they will be able to cover their tracks.[52]

These implications are especially concerning, and they carry far more national security risk if the attacker is an adversary nation state. A significant number of cyber

---

48 Proposed Rule for Investment Advisers and Funds, *supra* note 2, at 13539; Proposed Rule for Public Companies, *supra* note 3, at 16595; Proposed Rule for Market Entities, *supra* note 4, at 20257-58.

49 *See* Ari Schwartz, *The SEC Obstructs National Security*, WALL ST. J. (Sep. 30, 2022); Charlie Mitchell, *Tech sector cites need for incident reporting flexibility, law enforcement exemptions in SEC cyber rule*, INSIDE CYBERSECURITY (Sep. 08, 2022).

50 Schwartz, *supra* note 49; Mitchell, *supra* note 49 (quoting the Information Technology Industry Council).

51 *See* Schwartz, *supra* note 49; Mitchell, *supra* note 49.

52 Schwartz, *supra* note 49.

attacks have been carried out against the U.S. government and U.S. corporations in the past several decades, and the cyber capabilities of adversary states such as China, Russia, Iran, and North Korea only continues to grow.[53] Successful attribution is a vital piece of determining how to appropriately respond to such offenses, as is discovering intent – whether it be corporate information theft, a targeted financial attack, or preparing the virtual battlefield for a much larger offense.[54] Alerting such sophisticated actors that their attacks have been discovered risks successfully determining either.

Additionally, the proposed rapid, public disclosure could harm investors and shareholders by distorting the price of securities. Although the SEC's stated intention is to accurately inform stakeholders of companies' cybersecurity risk, the proposed rules force companies to contradict best practices, which increases the likelihood of additional attacks.[55] This premature public disclosure of an "uncontained or unmitigated incident may provide investors with an inaccurate measure of the registrant company's true ability to respond to cybersecurity incidents."[56] Requiring disclosure at such an early stage of the cybersecurity incident response could actually "result in investors receiving inaccurate information about the scope or impact of the incident" – the exact opposite of the SEC's stated aims.[57]

C. Dangers Posed by Cybersecurity Reporting Overlap

Another area of concern is the effect of adding to the already complicated system of regulatory reporting required by other federal and state entities. Because these proposed

---

53 *See generally* OFF. OF THE DIR. OF NAT'L INTEL., *supra* note 5 (noting the cyber capabilities of select adversary states).

54 *See generally* William Banks, *Cyber Attribution and State Responsibility*, 97 INT'L L. STUD. 1039 (2021) (discussing the importance and difficulty of cyber attribution).

55 Mitchell, *supra* note 49.

56 Mitchell, *supra* note 49.

57 *See* Mitchell, *supra* note 49.

rules are lengthy and relatively recent, their impact on each other and potential overlap is not yet understood. Among those to raise concerns are SEC Commissioners Hester Peirce and Mark Uyeda,[58] major trade groups,[59] the former special assistant to the president for cybersecurity policy,[60] and more. The confusion and potential mistakes stemming from the proposed rules' overlap with each other and existing regulations has the potential for negative unintended consequences.

A single company could conceivably be required to provide reports to the SEC within four days;[61] the Cybersecurity & Infrastructure Security Agency (CISA) within one to three days, depending on the nature of the incident;[62] the New York State Department of Financial Services in three days;[63] and the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corp. within thirty-six hours.[64] Companies working in multiple states and countries could be subject to an even more labyrinthine reporting regime, to say nothing of voluntary reporting.[65] Due to the uncoordinated nature of cybersecurity incident

---

58 Commissioner Peirce, *supra* note 44 ("the Commission has apparently decided...that a firm dealing with a cybersecurity attack first and repeatedly attend to the Commission's voracious hunger for data"); Commissioner Mark T. Uyeda, U.S. SEC. AND EXCH. COMM'N., *Statement on the Proposed Amendments to Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information*, Statement (Mar. 15, 2023), https://www.sec.gov/news/statement/uyeda-statement-regulation-sp-031523 ("The lack of an integrated regulatory structure may even weaken cybersecurity protection by diverting attention to satisfy multiple overlapping regulatory regimes...").

59 Mitchell, *supra* note 49.

60 Schwartz *supra* note 49.

61 Proposed Rule for Public Companies, *supra* note 3, at 16595.

62 *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Mar. 2022), https://www.cisa.gov/sites/default/files/2023-01/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf.

63 Schwartz, *supra* note 49.

64 *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, OFF. OF THE COMPTROLLER OF THE CURRENCY, FED. RSRV. SYS., AND FED. DEPOSIT INS. CORP., (Nov. 18, 2021), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf.

65 *See generally CyberIncident Reporting: A Unified Message for Reporting to the Federal Government*, DEPT. OF HOMELAND SEC., https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf (last visited May 14, 2023) (listing several government agencies to submit voluntary reports to).

oversight, this tangled web could easily cause confusion over which agencies to report to, what to report, and when reports are due. In addition to the administrative burden this causes, it could result in companies prioritizing reporting to entities that cannot help them over those that could provide tangible cybersecurity support, thus exacerbating the issue for fear of legal consequence.

D. Is the SEC the Best Actor to Receive this Information?

Underpinning the potential soundness of the proposed rules' reporting requirements is the question of what the SEC can and will do with any information received. Unlike reporting to CISA – an organization staffed with cybersecurity professionals, specifically created to act as the "operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience" – or other organizations with specialized cybersecurity capabilities, it is unclear what assistance the SEC could provide to a company undergoing a cybersecurity incident.[66] As pointed out by Commissioner Uyeda, "The SEC does not have a cyber response team that could immediately respond to seal the breach and provide technical assistance."[67]

Although the SEC has stated that the importance of quick reporting requirements, such as the forty-eight hour clock, is to allow the Commission to prevent "contagion" spreading to other actors in the same market segment, the SEC does not elaborate on how it would "reduce the probability of a contagion effect taking place."[68] While some cyber intrusions are the result of utilizing "zero-day" exploits or other malware that require

---

66 *See About CISA*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/about (last visited Apr. 23, 2023); *CISA Central*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/cisa-central (last visited Apr. 23, 2023).

67 Commissioner Uyeda, *supra* note 58.

68 Mulholland, *supra* note 15; Proposed Rule for Investment Advisers and Funds, *supra* note 2, at 13536 (failing to elaborate on what the SEC would do after "identifying patterns and trends across registrants").

cyber expertise to properly identify and repair, many are the successful outcome of techniques such as phishing that rely on human error.[69] The SEC does not seem well placed to deal with the former, and reminding an entire sector to protect against the latter does not promise large dividends. Any specialized knowledge that could help would need to come from an experienced cybersecurity source.

If the reported information does not allow the SEC to assist the afflicted company or the affected industry in any meaningful way, and the result of immediate, public disclosure could actually result in harm to the shareholders, perhaps there is a better way for the Commission to gain situational awareness of the situation than to receive direct reporting.

IV. Conclusion

The SEC's three proposed rules, as they are currently written, pose a danger to the cybersecurity well-being of corporations and would have a negative effect on their stakeholders and national security. The requirement to publicly report cybersecurity incidents shortly after their discovery, even if the cybersecurity incident is still ongoing, could result in additional cyber attacks, increased difficulty in attack attribution, and misinformed shareholders. The SEC does not provide a compelling reason why it requires this information so quickly, nor why it would be made public at the time it is received.

Potential solutions may include allowing companies to resolve cybersecurity incidents before making a report or keeping all reporting private until the cybersecurity incident has ended.

---

[69] *See generally Cyber Threats and Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories (last visited Apr. 23, 2023); *The 3 Main Types of Cyberattacks & How to Prevent Them*, CDW, https://www.cdw.com/content/cdw/en/articles/security/types-of-cybersecurity-threats.html (last visited Apr. 23, 2023) (detailing different types of cyberattacks and how to prevent them).

Either option should be specifically laid out in any final rule and not subject to change. Additionally, cybersecurity incident reporting among government agencies should be centralized and streamlined. Although the SEC does not have the power to do so itself, it could collaborate with other agencies, such as CISA, to simplify reporting procedures and allow companies to submit reports and receive assistance through the same mechanism.

While the SEC's three proposed rules – the Proposed Rule for Investment Advisers and Funds, the Proposed Rule for Public Companies, and the Proposed Rule for Market Entities – were all created with valuable foundations and positive intentions, they risk incidentally causing real harm due to their immediate, public reporting requirements. The reporting regime for cybersecurity incidents should be amended before a final rule is released to prevent this danger.