CYBER STATECRAFT INITIATIVE

DFRLab

#ACcyber

ISSUE BRIEF

JUNE 2023

Who's Afraid of the SEC?

The value in proposed rules for public cybersecurity incident disclosure

MAIA HAMIN

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

EXECUTIVE SUMMARY

New rules proposed by the US Securities and Exchange Commission (SEC) would require publicly traded companies to disclose cybersecurity incidents in public filings within days of their discovery. These rules have received pushback from commenters concerned about their impact on national security[1] and the potential duplication of a forthcoming requirement under the 2022 Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) to report incidents in critical infrastructure sectors to the federal government.[2] However, the SEC's proposed disclosure rules differ from the CIRCIA requirements—differences that offer material benefits not only for investors but for the broader cybersecurity ecosystem through the provision of publicly accessible and standardized data about cyber incidents.

The proposed SEC rule is an important, and distinct, complement to the CIRCIA requirements. The SEC's rule's combination of public disclosure, broad applicability, and standardized reporting—coupled with enforcement by a well-resourced federal agency—will provide a level of cybersecurity transparency that is more robust than existing incident disclosure requirements, including state-level data breach laws and sector-specific reporting requirements.

A higher level of transparency would benefit the overall health of the cybersecurity ecosystem by improving information asymmetries in the cybersecurity market for companies and consumers, allowing regulators to more efficiently employ existing policy tools, and supporting research. In turn, this could cata-

1 Ari Schwartz, "The Securities and Exchange Commission Obstructs National Security," *The Wall Street Journal,* September 29, 2022, https://www.wsj.com/articles/the-sec-obstructs-national-security-cyber-attack-defense-corporations-cybersecurity-china-india-public-disclosure-report-11664487542.

2 ACA Connects et al., "Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File Number S7-09-22)," June 22, 2022, https://www.sec.gov/comments/s7-09-22/s70922-20132693-303184.pdf.

lyze better cybersecurity behavior by shifting incentives and making the cyber landscape more legible for consumers, businesses, and policymakers.

The brief evaluates the SEC proposal and common points of criticism before suggesting remedies to address these concerns while preserving the important potential benefits. In light of the renewed national conversation about market failures in cybersecurity stemming from the 2023 National Cybersecurity Strategy, the cybersecurity community should embrace this unique moment of opportunity where an existing regulator has both the authority and the will to implement changes with far-reaching potential benefits.

INTRODUCTION

The SEC has broad authority to require public companies to make routine disclosures of facts that are materially relevant to investors who own or may buy stock in publicly traded companies. In March of 2022, the Commission released a notice of proposed rulemaking (NPRM) related to cybersecurity practices and risk management at public companies.[3] The proposal was re-opened for comment in March of 2023 and closed on May 22.

While the proposed rules included several changes to existing policy, including requirements to disclose information about the cyber expertise of a company's board and its cybersecurity risk management strategy, one requirement has risen above all others in the discussion: incident disclosure. This provision would require public companies to disclose cybersecurity incidents within four days of determining that they could be significant to investors. The SEC's justification for this rule is straightforward: investors have an interest in understanding whether and when a publicly traded company has been impacted by a cyber incident because these incidents can have material financial and reputational effects on a company, including costs due to interruptions in business, ransom payments, and investigation and remediation, as well as litigation risks and increased insurance premiums.[4] As such, the rule is well within the SEC's conventional authority. However, along with the more traditional pushback on any new reporting requirements, the stringency of the mandated reporting timeline has drawn attention from experts.

Existing incident disclosure requirements include state-level data breach laws, sector-specific requirements imposed by regulatory agencies, and a forthcoming provision for critical infrastructure sectors to report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) under CIRCIA. Many of these laws have different focuses and intentions, including informing consumers when their data has been breached (state level) so that they can take steps to prevent identity theft, or informing regulators of an incident for risk-management purposes (most federal-level requirements).

There is an ongoing debate about the precise degree to which data breach or cyber incident disclosure requirements drive better cybersecurity market behavior, but research does appear to show that disclosure requirements can encourage companies to invest more in cybersecurity and reduce future cyber risk.[5] From this perspective, this issue brief argues that the proposed SEC rules are important because they provide a mechanism for public transparency around cyber incidents that is meaningfully distinct from any existing disclosure requirements, uniquely combining:

- A requirement for public disclosure
- Broad applicability to a range of sectors and types of cyber incidents
- Standardized reporting requirements under a single agency
- Enforcement by a well-resourced federal regulator

Taken together, these factors make the SEC's proposal uniquely valuable to the broader cybersecurity market and policymaking activities that require usable and meaningful data on incidents and breaches.

EXISTING INCIDENT DISCLOSURE REQUIREMENTS

State data breach laws

All fifty states have some version of a "data breach law" that places certain obligations on companies after the improper exposure—whether malicious or unintentional—of data.[6] Generally, these laws are triggered by breaches of personal data (data that pertains to and uniquely identifies an individual) of state residents. These laws typically require that companies disclose to state residents that their information was breached and sometimes mandate additional reporting of incidents of a certain size or

3 "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," SEC, March 9, 2022, https://www.sec.gov/news/press-release/2022-39.

4 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Federal Register, March 23, 2022, https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure.

5 Musaib Ashraf and Jayanthi Sunder, "Can Shareholders Benefit from Consumer Protection Disclosure Mandates? Evidence from Data Breach Disclosure Laws," *The Accounting Review*, February 17, 2023, 1–32, https://doi.org/10.2308/TAR-2020-0787; Joseph Buckman et al., "Do organizations learn from a data breach?," Workshop on the Economics of Information Security, 2017, https://weis2018.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_55.pdf.

6 "Security Breach Notification Laws," National Conference of State Legislatures, January 17, 2022, https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.

severity to the state's Attorney General.[7] Some states, such as California, also post notices of large-scale data breaches to a public website.[8]

These notification requirements amount to something like a public disclosure requirement, if through an indirect mechanism: if consumers are receiving letters about a data breach, it is difficult to keep the story out of the news. State-level disclosure laws generally have laxer timelines than those proposed by the SEC. Most vary from thirty to sixty days after the incident was discovered and allow for delays to address the breach or at the request of law enforcement. It is difficult to understand from public data the frequency of these exceptions and how much they delay notification.

It is also difficult to measure companies' compliance with state-level data breach requirements. Surveys of cybersecurity managers and professionals are not promising: a 2019 study found that half of the participants believed that enterprises underreport cybercrime, even when legally required to do so,[9] and another in 2023 found that 72 percent of respondents who had experienced a data breach did not disclose the incident.[10]

One possible reason for this underreporting is that the potential penalties for failing to disclose incidents are often smaller than the expected costs of reporting and publicly revealing data breaches. Most state laws cap penalties for non-compliance at $1 million (with many much lower),[11] while the average cost of a data breach in the US is approximately $9 million.[12] Disclosing data breaches creates costs for companies in the form of delivering notifications and providing redress such as identity monitoring, as well as through the threat of future fines for insufficient security practices.[13] As such, companies may examine this tradeoff and decide to take their chances on flying under the radar.

Sector-specific incident reporting requirements

Some sectors have specific cyber incident reporting requirements. For example, the Health Insurance Portability and Accountability Act's (HIPAA's) Breach Notification Rule,[14] as well as rules enforced by the Federal Trade Commission (FTC),[15] require health care providers and record vendors to disclose health information breaches to consumers and the Department of Health and Human Services (HHS) or the FTC. While health care breaches that affect more than five-hundred individuals must be reported to HHS and publicly posted on a website or in the media, small incidents can be reported annually with few specific details.[16] Many financial services companies are also subject to incident reporting requirements. According to a 2022 rule created by the Federal Deposit Insurance Corporation (FDIC) and the Federal Reserve, financial institutions such as banks must notify their regulators within thirty-six hours of a serious data breach, though they are not obliged to inform counterparties, customers, or the public at large.[17]

These sector-specific laws have a noticeable effect: companies in highly-regulated sectors such as healthcare and finance reportedly pay much higher costs associated with data breaches than their less-regulated counterparts.[18] However, these regulations apply to a relatively limited swath of the economy compared to the SEC's proposed rules. For example, of the 7,640 companies listed on one of the US-based Nasdaq, NYSE, or AMEX exchanges, only 1,302 are in the health care sector and 2,023 in the financial sector,[19] leaving many public businesses that are not subject to any federal-level incident reporting requirements.

Preexisting SEC cybersecurity reporting requirements

The SEC has no existing reporting requirements related to cybersecurity incidents. However, the Commission has issued interpretive guidance regarding the application of existing non-cyber disclosure requirements to cybersecurity incidents. In particular, its 2018 Interpretive Release states that companies should consider the materiality of cybersecurity risks and incidents for existing registration statements and periodic reports. The Interpretive Release outlines several existing disclosure requirements for which cybersecurity incidents might be material, such as in descriptions of businesses and their financial situations or disclosures related to legal proceedings.[20] In its NPRM, the SEC addresses these requirements, stating that, while many companies report cybersecurity incidents in such disclosures, the Commission's staff have identified cyber incidents reported in the media which were not included in filings. In addition, the NPRM

7 "Data Breach Notification Laws by State," IT Governance USA, July 2018, https://itgovernanceusa.com/data-breach-notification-laws.

8 "Search Data Security Breaches," State of California Department of Justice - Office of the Attorney General, accessed May 25, 2023, https://oag.ca.gov/privacy/databreach/list.

9 "New Study Reveals Cybercrime May Be Widely Underreported—Even When Laws Mandate Disclosure," ISACA, https://www.isaca.org/about-us/newsroom/press-releases/2019/new-study-reveals-cybercrime-may-be-widely-underreported-even-when-laws-mandate-disclosure.

10 *The State of Cybersecurity 2023,* Arctic Wolf, accessed May 25, 2023, https://cdn.pathfactory.com/assets/10926/contents/482399/7f7a4fcc-f0c7-495f-bd1b-a1922aad2ccc.pdf#pdfjs.action=download.

11 "The Ultimate Guide to Data Breach Laws By State," Embroker, January 2, 2023, https://www.embroker.com/blog/data-breach-laws-by-state/.

12 "Cost of a Data Breach 2022," IBM, July 2022, https://www.ibm.com/reports/data-breach.

13 "Cost of a Data Breach 2022."

14 45 CFR § 164.400-414, https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164.

15 The Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub.L. 123 Stat. 227 (2009)

16 "Breach Notification Rule," HHS, July 26, 2013, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

17 Carter Pape, "7 data breach reporting rules banks need to understand," *American Banker*, May 19, 2022, https://www.americanbanker.com/list/7-data-breach-reporting-rules-banks-need-to-understand.

18 "Cost of a Data Breach 2022."

19 "Stock Screener," Nasdaq, accessed June 1, 2023, https://www.nasdaq.com/market-activity/stocks/screener.

20 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,"

notes the vast range in the scope and detail of information that companies provide about cybersecurity incidents even when they choose disclosure. Acknowledging this reality, the SEC justifies its new rules by noting that existing reporting "is inconsistent, may not be timely, and can be difficult to locate."[21]

CIRCIA

The 2022 Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) will require entities in critical infrastructure sectors to report cyber incidents to CISA within seventy-two hours.[22] CISA has until March of 2024 to issue proposed rules to implement CIRCIA and define what kinds of "substantial cyber events" a "covered entity" must report.[23] Covered entities must be in critical infrastructure sectors, those whose incapacity or destruction would have a "debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[24] This could include companies operating in the energy, transportation, health care, defense, information technology, and financial services sectors.

CIRCIA requires reporting only for incidents that involve a "substantial" loss of confidentiality, integrity, or availability; cause disruption to business or industrial operations; or involve supply chain attacks or compromise through a third party, such as a cloud service provider.[25] Such a definition would include losses of operational functionality (such as in the Colonial Pipeline ransomware incident)[26] and should, ideally, also include data breaches that might impact national security (such as a recent breach of the DC Health Link data exchange, which exposed the personal information of members of Congress and staffers).[27]

While CIRCIA requires entities to report covered incidents to CISA, it does not mandate public disclosures. The legislation does require CISA to "publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations based on covered cyber incident reports," and to "proactively identify opportunities [...] to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable."[28]

These reports and research opportunities will ideally ensure that information provided by this new requirement does not stay wholly within the cloisters of government. However, aggregated and anonymized data will not create accountability for individual companies, nor support additional research beyond what is already internally conducted by CISA. Sharing government-held data for cybersecurity research purposes is a thornier proposition than it may seem, with "complicated, unclear processes for delineating how data can be accessed and used" having long frustrated researchers seeking to access information held by federal agencies in other contexts.[29]

THE PROPOSED RULES

When?

The SEC's proposed rules require public companies to report "material cybersecurity incidents" through a Form 8-K (a type of immediate disclosure a company must file for types of events the SEC has determined are too time-sensitive to wait for quarterly or annual filings). In general, companies have four business days to file Form 8-Ks for other events—likely the precedent driving the proposed four-day timeline for incident disclosures.

An important distinction for cybersecurity incidents in particular is that companies must file a Form 8-K within four business days of the day they determined the *materiality* of the incident, not from the day of discovery. The SEC states that it expects some companies will be able to determine that a cyber incident was material on the same day they discover it, while others may take longer. It is important to note that companies do not need to fully investigate or remediate a breach to determine materiality. Per the SEC's guidance, materiality will hinge on whether it is likely a shareholder in the company would consider the incident important for making an investment decision or if the incident alters the "total mix" of available information.[30] Practically, this means that once a company discovers that an incident had significant impacts, such as the loss of data, the four-day reporting requirement is triggered regardless of whether the company understands how its systems were breached.

21 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."

22 "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," CISA," accessed May 24, 2023, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

23 Cyber Incident Reporting for Critical Infrastructure Act of 2022, 6 U.S.C. §618; "Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022," Federal Register, September 12, 2022, https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022.

24 President Barack Obama, "Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience," The White House, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

25 Cyber Incident Reporting for Critical Infrastructure Act of 2022.

26 "Colonial Pipeline Cyber Incident," US Department of Energy, accessed May 25, 2023, https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.

27 Justin Papp, "Officials Probe DC Health Link Breach That Exposed Hill Staff Data," *Roll Call*, March 9, 2023, https://www.rollcall.com/2023/03/09/officials-probe-dc-health-link-breach-that-exposed-hill-staff-data/.

28 Cyber Incident Reporting for Critical Infrastructure Act of 2022.

29 Nick Hart and Kody Carmody, *Barriers to Using Government Data: Extended Analysis of the U.S. Commission on Evidence-Based Policymaking's Survey of Federal Agencies and Offices,* Bipartisan Policy Center, October 10, 2018, https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2018/10/Barriers-to-Using-Government-Data.pdf.

30 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."

Naturally, this raises the question of whether companies will intentionally slow down their investigation of a cyber incident in hopes of delaying notification. The SEC anticipates this issue, and, to "address any concern that some registrants may delay making such a determination to avoid a disclosure obligation," instructs that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."[31] This brief addresses this topic in more detail below, suggesting the SEC consider adding a requirement to disclose a timeline of an incident and its discovery to further disincentivize companies from dragging their feet on determining materiality.

When... not?

The proposed rules offer no exceptions to the four-day disclosure requirement. This includes no exceptions for ongoing incidents, nor for preventing potential interference in an active law enforcement investigation. Notably, there is not even a disclosure exception for incidents that could potentially harm national security. The SEC, in its NRPM, asked commenters to consider whether it should include an exception allowing the Attorney General to delay notification to prevent potential harm to US national security but did not include the exception in the proposed rules.33 This total lack of exceptions is the most controversial component of the new proposed rule and the topic of many comments responding to the SEC's NPRM.

What?

The rules define a "cybersecurity incident" as "an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein." Taken in combination with the materiality standard, this definition encompasses a relatively wide range of cyber incidents. Indeed, the SEC gives examples of cyber incidents that would likely be considered material, which include everything from intentional and unintentional breaches of personal data to hacks that interfere with company operations, the theft of company intellectual property, and ransomware.[32]

The SEC proposal requires a company to disclose several facts about an incident:

- "When the incident was discovered and whether it is ongoing;
- A brief description of the nature and scope of the incident;
- Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
- The effect of the incident on the registrant's operations; and
- Whether the registrant has remediated or is currently remediating the incident."[33]

The SEC clarifies they would "not expect a registrant to publicly disclose specific, technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident."[34] The SEC also recognizes the fact that, only four days after a breach is deemed material, companies may have imperfect information, and states that any "material changes or updates" should be included in quarterly and annual filings (Forms 10-Q and 10-K, respectively).

From the perspective of the SEC, this set of data makes sense: it focuses on information essential to investors to assess a company's financial outlook while minimizing the risk that the disclosure will provide a playbook for other attackers. How the inclusion of additional information about the *incident itself* could serve both investors and the general cybersecurity ecosystem is addressed near the end of this paper.

WHAT ARE THE BENEFITS OF THE NEW SEC RULES?

The proposed SEC incident disclosure requirements, by improving transparency, would provide meaningful benefits to the technology marketplace, enterprises, and individuals alike, complementing CIRCIA and state-level laws. These benefits are:

1. Incident disclosures would be made public (unlike, for the most part, CIRCIA) on a rapid timeline (unlike both state-level laws and CIRCIA).
2. Disclosure is required for a broad range of cybersecurity incidents, including the theft of personal data, intellectual property data, or data with potential national security implications (broader than both CIRCIA and state-level laws as well as addressing a major national security issue).[35]
3. Standardized reporting requirements will provide a single resource for reports, benefiting consumers and researchers (unlike state-level data breach disclosures, many of which are not publicly posted, let alone in a single location).

31 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."
32 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."
33 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."
34 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."
35 *Annual Threat Assessment of the U.S. Intelligence Community,* ODNI, February 26, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

4. Enforcement by a well-resourced federal regulator with the ability to levy large fines may incentivize compliance (compared to state Attorneys General, who often lack the resources or authority to extract significant monetary penalties).

Though the SEC's specific goal for these rules is protecting investors, a federal requirement to publicly disclose cyber incidents could have strong secondary benefits by increasing overall transparency in the cybersecurity ecosystem. Several of these potential benefits are outlined below.

1. Addressing information asymmetries

The cybersecurity market suffers from information asymmetries—it is often difficult for buyers and users to evaluate the security of products, meaning they cannot make purchasing decisions on the basis of cybersecurity. This asymmetry then disincentivizes businesses from investing in cybersecurity, as security investments create costs without commensurate benefits in terms of attracting more customers or raising prices for services and products.

A historical dataset of cyber incidents at public companies would allow potential consumers or counterparties to evaluate a company's cybersecurity track record and compare businesses across similar sectors and operating environments. In turn, this could drive companies to invest more in cybersecurity, as their consumers and counterparties could more accurately incorporate cybersecurity as a factor in their purchasing decisions. Consumers may benefit from having information to evaluate the cybersecurity practices of a potential provider before handing over their personal financial data or installing a smart-home application. Business counterparties, on the other hand, might want to understand a partner's history of breaches before integrating their software into their enterprise network. Thus far, such information has been unevenly available in the cyber ecosystem.

The advantage of such a requirement at the federal level is that it will standardize information about disclosures in form and location, facilitating easier downstream use. Existing state-level requirements vary on whether and where information is publicly posted, making it difficult to establish a consistent baseline when businesses may operate in different states and report to different authorities. In contrast, standardized and up-to-date information from SEC filings about potential breaches would provide a source for aggregation by third parties such as consumer watchdogs or consulting firms that compile risk assessments for businesses' supply-chain decisions.

Enshrining a broad, standardized disclosure requirement would also help transform incentive structures that encourage obfuscation over disclosure. In an ecosystem where only some companies choose to disclose a data breach, there may be a perverse effect in which companies that attempt to be more transparent are seen as "less secure" because consumers hear about their cyber incidents. Meanwhile, tight-lipped competitors might be perceived as more secure, even if they have had more breaches. Required disclosure, backed up by powerful enforcement, can alter the incentives for companies to hide cyber incidents and hopefully move the broader ecosystem to further embrace norms of transparency.

2. Strengthening existing enforcement mechanisms

The SEC's proposed rule is merely a disclosure requirement—it does not imply that companies that disclose a cyber incident have necessarily done something wrong. However, a public incident notification would also alert other entities with the authority to ensure the company lived up to its obligations to protect customers and investors from cyber risk. For example, a disclosure could tip off states' Attorneys General, who have the authority to investigate whether a company was compliant with the standards of state data breach laws in its handling of personal information, or the FTC, which can investigate companies that may have misrepresented their security practices. A public notice could also catch the eye of customers of the company, who might seek redress through mechanisms like a class action lawsuit. Investors may also want to hold companies to account for securities fraud if they believe the company misrepresented its cybersecurity protections or maturity. All these possibilities require that interested parties know about the cyber incident.

This potential benefit is based on the presumption that SEC reporting requirements will result in the public disclosure of a broader set of incidents than companies currently disclose. This seems likely, in part due to the proposed rules' relatively expansive definition of a cyber incident, which is not limited to personal data or based on a company's knowledge that the data pertains to residents of certain states. Additionally, if it is true that public companies are under-disclosing data breaches, the threat of potential SEC enforcement action is likely a stronger disincentive than existing penalties for nonreporting. Indeed, the SEC has the authority—and resources—to levy much larger fines and has already obtained multi-million settlements against companies for issuing misleading disclosures about data breaches.[36] This fact should weigh heavily on the minds of decision-makers within companies as they evaluate the cost-benefit tradeoff of disclosure.

36 "Yahoo Agrees to $35 Million SEC Penalty Over Cyber Incident," Paul, Weiss, Rifkind, Wharton & Garrison LLP, May 3, 2018, https://www.paulweiss.com/practices/transactional/capital-markets/publications/yahoo-agrees-to-35-million-sec-penalty-for-failure-to-disclose-cyber-incident?id=26363; "SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors," SEC, March 9, 2023, https://www.sec.gov/news/press-release/2023-48.

3. Providing crucial data about the cyber ecosystem for research and policymaking

More public data on cybersecurity incidents would help not only investors and customers but benefit researchers, regulators, and policymakers who need data on breaches and cyber incidents to inform policy and practice. Right now, researchers and policymakers have poor visibility into the occurrence of cyber incidents in the US. Attempting to understand the different types of cyber incidents, how often they occur, and their effects requires piecing together media reports and state- or sector-specific disclosure notices, forming a deeply incomplete picture. In 2020, the bipartisan congressionally mandated Cyberspace Solarium Commission (CSC) found that:

> *"While there is broad consensus that cyberattacks on U.S. citizens and businesses are increasing in frequency and severity, the U.S. government and broader marketplace lack sufficient clarity about the nature and scope of these attacks to develop nuanced and effective policy responses. Compounding this problem is a fundamental lack of clarity about what security measures are effective in reducing risk in the technologies, in business enterprises, and even at the level of national policymaking. This confusion limits the ability of the government to evaluate the effectiveness of its cybersecurity programs and prevents private enterprises and insurance providers from being able to adequately price, model, and understand cyber risk. Existing data sets are incomplete and provide only a superficial or cursory understanding of evolving trends in cybersecurity and cyberspace."*[37]

To address this challenge, the CSC recommended the creation of a Bureau of Cyber Statistics to capture and report data for government and private sector use. Nearly three years later, neither this nor similar recommendations have been enacted into law.

SEC disclosures could begin to help fill this information gap. The proposed SEC rules would create a centralized data resource on cyber incidents for researchers and, unlike incidents reported under CIRCIA, these disclosures would be public. This would allow academics, consumer safety groups, insurers, and other private sector entities to use the data without submitting Freedom of Information Act (FOIA) requests or gaining entry to special information sharing programs. While the form of SEC disclosures might not be granular enough to answer all research questions—for example, companies do not need to disclose details of an attacker's tactics, techniques, and procedures—improved visibility into the prevalence and frequency of cyber incidents would still be a significant improvement over the status quo, where data (and thus a picture of the relative efficacy of policy interventions) is still scarce.

A PATH FORWARD

Considering these benefits, the SEC should push forward with its rulemaking while responding to valid criticisms of the current language. The following section addresses these critiques and offers potential solutions.

Timeline, law enforcement, and national security

Many of the comments on the SEC's NPRM focus on the short length of the four-day disclosure window and that the timeline applies whether the incident has been fully contained and remediated. For example, Rapid7, a cybersecurity company, advised that "public disclosure of an unmitigated or uncontained cyber incident will likely lead to attacker behaviors that cause additional harm to investors," including attack escalation (e.g., more aggressive exfiltration of data) and anti-forensic activity (e.g., deleting activity logs). Rapid7 also warned that this could lead to copycat attacks by other malicious actors seeking to exploit the same vulnerability.[38] Nasdaq, speaking on behalf of many listed participants, stated in its comment that "feedback indicated that the four business day timeframe (1) may interfere with a public company's primary obligation to remediate a cybersecurity intrusion; and (2) is an exceptionally short time period in which to understand the nature and scope of a cybersecurity breach as well as its potential impact."[39] Many other comments on the NPRM share these concerns.

The SEC proposes that delaying reporting on an active cyber incident is a potential solution for these issues, but ultimately determines that lengthy investigations would leave investors in the dark for too long. An additional issue—perhaps one the SEC thought too delicate to raise directly—is that allowing companies to delay notification during remediation could be counterproductive to security, as companies may drag their feet to postpone disclosure.

Another set of objections to the SEC reporting requirements is that they make no exceptions for cyber incidents of national security or law enforcement interest. Here, the fear is that the rapid disclosure of certain types of incidents could have detrimental effects on US national security or impede law enforcement investigations.

37 *U.S. Cyberspace Solarium Commission Final Report*, U.S. Cyberspace Solarium Commission, March 2020, https://www.solarium.gov/report.

38 "Comments to the Securities and Exchange Commission," Rapid7, August 29, 2022, https://www.sec.gov/comments/s7-09-22/s70922-20137661-308069.pdf.

39 John. A. Zecca, "File No. S7-09-22, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Nasdaq, May 9, 2022, https://www.sec.gov/comments/s7-09-22/s70922-20147083-312666.pdf.

These concerns are important to address while balancing investors' interests. The SEC must ensure that reporting exceptions can be used when necessary while preventing abuse and perverse incentives that might create unnecessary delays in informing investors. There are historical reasons to be skeptical of open-ended reporting delays for mitigation, law enforcement, or national security purposes. The CEO of Equifax, Richard Smith, offered few specifics in a Congressional hearing when asked why his company delayed notifying consumers for more than a month that their sensitive credit data was stolen and whether law enforcement had asked the company to delay reporting.[40]

Recommendation One: Allow companies to delay reporting for ongoing or uncontained cyber incidents but create a hard maximum deadline for reporting thirty days after the incident is determined to be material.

As suggested by Rapid7, a thirty-day period should be sufficient to investigate and remediate the vast majority of cyber incidents.[41] This would give companies time to secure their systems and to preserve evidence—addressing concerns about the destruction of evidence relevant to law enforcement investigations while ensuring companies must disclose in a timely fashion after a threat is contained. In addition to setting such a maximum, the SEC could improve the timeliness of reporting by focusing on exceptions for ongoing or uncontained incidents rather than allowing companies to delay notification during the entire investigatory period. While the SEC must also consider investors' concerns, even thirty-day-old data would be a significant benefit to the broader cybersecurity ecosystem.

Recommendation Two: Allow companies to delay notification when reporting would have a negative effect on national security as certified by the Attorney General or CISA. Implement a non-waivable maximum delay for these exceptions.

The SEC has already asked commenters whether it should allow the Attorney General to delay a notification based on national security concerns.[42] Such a process could also leverage the forthcoming CIRCIA requirements to report national security-relevant cyber incidents to CISA, which would provide a natural opportunity for CISA or the Department of Homeland Security to issue a waiver if the disclosure of an incident would harm US national security. This delay could also be subject to a maximum cap of thirty days.

The next section recommends additional transparency measures to enable oversight for disclosure exceptions and more strongly align incentives for companies to inform investors as soon as possible after a cyber incident.

Information content of disclosures

The SEC could provide additional benefits to investors and the broader ecosystem by standardizing the information companies must provide about an incident in quarterly filings. As the rule currently stands, the disclosure is focused more on the effects of the incident on the company than on its nature or cause. Companies may have a fair amount of flexibility to define what is included in "a brief summary of the nature and scope of the incident"[43] and are unlikely to volunteer detailed, standardized information about the incident's timeline unless required by the SEC.

The SEC could require more detailed descriptions of an incident and its timeline to enable investors and the public to better predict a company's future level of cybersecurity risk. Investors and potential customers should rightfully consider differently a company that took a year to discover an intrusion and months to remove attackers versus one which identified and remediated an incident rapidly, or a company that was exploited through unpatched servers versus through a novel attack vector. This additional information would be timely and relevant, as the SEC's rulemaking is focused on informing the total mix of information available to investors evaluating both current *and* future costs associated with a company's cybersecurity posture.

For researchers and policymakers, this information would create more usable, public data about cybersecurity practices, critical product classes, and sector-specific trends in cybersecurity outcomes. This data could also inform future research and policy initiatives to shore up components of the cybersecurity ecosystem that have been weak links in real-life breaches. Additionally, if companies must provide an account of the incident's stages from occurrence to discovery, investigation, and mitigation, they will be more accountable to shareholders and the public for long-undiscovered incidents or sluggish remediation. Requiring companies to report the reason for a delayed notification could also bolster policymaker and public oversight of disclosure exceptions, furthering the SEC's goal of ensuring that notification is as timely as possible.

40 "Examining the Equifax Data Breach," US House of Representatives Committee on Financial Services, October 5, 2017, https://www.govinfo.gov/content/pkg/CHRG-115hhrg30242/html/CHRG-115hhrg30242.htm.

41 "Comments to the Securities and Exchange Commission," Rapid7.

42 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."

43 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."

Recommendation Three: Standardize quarterly reporting to include additional information about the nature of an attacker's path into and through affected systems and a timeline of the incident's occurrence, discovery, remediation, and disclosure.

The SEC has already suggested the possibility that additional information should be included in quarterly reporting, requiring companies to detail "any changes in the registrant's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes."[44] By adding required disclosures about an incident to quarterly reporting, the SEC can give businesses more time to investigate an incident and further appease concerns from companies, the government, and law enforcement about ongoing threats or potential national security effects.

NO MORE UNACCOUNTABILITY THROUGH OBSCURITY

Cybersecurity, for a field founded on the study of information systems, has always been peculiarly in the dark when it comes to high-quality, public data about cybersecurity incidents. Due to the myriad potential consequences in the form of liability, business losses, and public shame, companies often seek to hide and downplay cyber incidents. While these actions are often sensible from a business perspective, the status quo of secrecy blocks meaningful progress in re-aligning incentives in the cyber ecosystem.

Ultimately, companies are responsible for cybersecurity outcomes based on their practices and resourcing. Until the cost of bad outcomes becomes higher than the cost of investing in cybersecurity, the market will not reward different behavior. Transparency is a critical first step.

Increased public transparency for cyber incidents can help address information asymmetries that lead to market failures, jump-start enforcement mechanisms that are currently hamstrung by poor visibility, and inject much-needed data into the broader cyber ecosystem for researchers and regulators. Cybersecurity incidents have been shrouded in opacity for too long, at the expense of better-informed policymaking and practices. Even if it is not the primary goal of its rulemaking, the SEC has the tools at hand to reshape these dynamics and strengthen the cyber ecosystem.

ACKNOWLEDGEMENTS

Thank you to Josephine Wolff, Paul Rosenzweig, Sara Ann Brackett, Emma Schroeder, and Trey Herr for their feedback on various versions of this document.

44 "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Gina F. Adams
Timothy D. Adams
*Michael Andersson
Barbara Barrett
Colleen Bell
Sarah E. Beshar
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Jeff Shockey
Ali Jehangir Siddiqui
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of May 22, 2023