# New SEC Cybersecurity Disclosure Protocols: Enhanced Transparency, Short Deadlines

Brian Walker[1]

[1] Founder, The CAP Group, Brian@TheCAP.Group

Abstract

The Securities and Exchange Commission (SEC) issued its final rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Response on July 26, 2023. This mandates that SEC-regulated companies disclose both significant cybersecurity incidents and their cyber risk management processes. These public disclosures will be made via existing SEC reporting channels. They are intended to provide investors with enhanced transparency into the cyber risks and mitigation strategies employed by SEC-regulated corporations.

This landmark decision marks the culmination of an 18-month intensive rulemaking process that commenced in March 2022. The process was anything but smooth. The interval from the SEC's original announcement to the finalization of the rules was marked by fervent debate, heated public discourse, and diverging viewpoints.

Adapting to the new regulations will vary among companies. Established firms with robust practices will find the transition smoother, primarily focusing on initial disclosures for the year's 10-k report. In contrast, companies with less structured cyber risk approaches and reliant on reactive measures, will grapple with substantial challenges. Central to this transition is the collaboration between boards and executives in defining "material" cyber incidents. While no fixed formula exists to gauge impact, it is crucial for leadership to holistically understand and swiftly assess potential repercussions—spanning operational costs, legal ramifications, brand implications, and revenue loss—during emergent cyber situations.

## Introduction

The continuing surge of cybercrime in the U.S. has led to colossal financial losses, estimated in the hundreds of billions of dollars, posing not only a significant eco-

 doi: 10.18278/jcip.4.1.7

nomic threat but also jeopardizing public safety.[1] In a pivotal move to address this concern, on July 26, 2023, the SEC issued its final rules for companies disclosing key information regarding cyber risk.[2] The landmark decision marked the culmination of an 18-month intensive rulemaking process that commenced in March 2022.

The process was characterized by passionate public debate and discussion and a wide spectrum of perspectives. While a segment argued about the tangible benefits of such reporting, others questioned the SEC's jurisdiction in mandating the new disclosures. Furthermore, the discourse was rife with intricate discussions on defining terms and assigning responsibilities pertaining to cyber risks. Despite divergent opinions, the SEC addressed the majority of the concerns, culminating in finalization of the rules. As a result, companies are expected to align with these compliance norms starting December 2023.

## Annual Cyber Risk Disclosures

The rules as finalized in July are focused on the public disclosure of cyber risk information. There are two disclosure time horizons: annual and incident driven. On an annual basis, companies are required to incorporate new cyber-specific information in their SEC Form 10-k that addresses two general areas:

### *Cyber Risk Management*

This incorporates the strategies and processes used by the company in monitoring and managing cyber risk overall. This area is broadly focused on providing clarity into how a company thinks about cyber risk at-large and how it frames risks that originate in the cyber domain. They exist in the context of numerous other enterprise risks such as competition, regulation, financial/currency exposures, physical plant operations risks, etc.

### *Cyber Risk Governance*

These involve the professional backgrounds, roles, and responsibilities of those involved in monitoring and managing cyber risk. This area is focused on understanding the mechanics of how cyber risk is governed across the company. The governance focus includes both the board of directors and the executive leadership team. The original draft rules in 2022 included a requirement to reveal the names and biographies of key directors and officers who are viewed by a company

1 "The U.S. Is Less Prepared to Fight Cybercrime Than It Could Be," General Accounting Office, WatchBlog, August 29, 2023.

2 SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, U.S. Securities and Exchange Commission, Press Release, July 26, 2023.

as having credible cyber risk expertise. While the 2023 finalized rules omitted the board of directors from this mandate, it retained the emphasis on key executives. This move underscores the importance of leaders actively involved in cyber risk comprehension and mitigation.

These data are slated for release as a component of the traditional 10-k disclosure mechanism. The inaugural set of disclosures will be requisite for organizations scheduled to publicize their 10-k post-mid-December 2023. Note that the SEC did not provide detailed guidance on how to provide these disclosures. They did not mandate specific elements for inclusion, provided no lexicon/framework, and remained silent on the granularity of detail sought. The SEC's primary focus is transparency at-large—leaving the particulars to the discretion of each company's leadership.

## Incident Disclosures: A Closer Look

Beyond annual declarations, the SEC has decreed that enterprises disclose significant cyber-related incidents. Aligning with its stance on yearly revelations, the SEC refrained from outlining the criteria defining a material cyber incident. The notion of public disclosure of material incidents is not new, so the SEC will rely on existing case law and precedents for gauging the materiality of cyber incidents, just as companies have to evaluate the materiality of other business incidents such as natural disasters, currency fluctuations, factory fires, etc.

There is one nuance in incident disclosure where the SEC issued a prescriptive requirement—the timeliness of such disclosures. As per the SEC rules, companies must disclose material incidents within four business days of reaching the determination of materiality. Note that this is not four days from when the incident occurred or was discovered, but four days from when the determination of materiality has been completed. This is in alignment with other material non-cyber disclosures as the SEC seeks to treat cyber risks in similar fashion to all other business risks.

## Navigating Adoption Hurdles

The degree of difficulty in adopting these new rules will vary widely, based on a company's current level of sophistication in managing cyber risk. For large, sophisticated organizations with highly-developed cyber risk management capabilities, this adoption will require only modest effort—likely focused primarily on the initial release of information for inclusion in the first year's 10-k.

Companies with less structured cyber risk management practices are poised to encounter substantial adoption challenges. Historically, many of these firms have relied on a reactive, improvisational strategy, where the ingenuity and adaptability of their leadership play pivotal roles during cyber events. Those informal

and reactive methods are rarely documented in clear, concise terms, with unambiguous processes and roles that would give transparency and comfort to investors. For these firms, the fourth quarter of 2023 could require an intense first-time documentation of such practices with sufficient clarity—and legal approval—to be ready for formal disclosure in an SEC 10-k.

In addition to the mechanics of risk management and governance, there are key strategic decisions that must be made requiring the alignment of the board and the executive team. One key alignment is the definition of materiality. As part of an organization's risk management process, there needs to be agreement on the parameters of cyber risk that will be considered when evaluating a cyber incident. Typical considerations include the costs associated with technical resumption of operations, costs associated with litigation and fines, loss of brand goodwill, and unrecoverable lost revenue. Each incident may involve different portions of these and many other considerations, and an exact formula isn't feasible. However, it is feasible—and expected—that directors and officers understand the potential mix of impacts in determining materiality and that they align on the mechanics of rapidly evaluating these as a fast-moving cyber incident is unfolding.

## Crucial Areas of Focus

Compliance with the SEC rules will be based on key foundational capabilities that are not new but will be more visible given the transparency requirements. In parallel with drafting the materials for annual disclosure, it will be important to ensure that the underlying processes, tools, and capabilities are sufficiently robust to enable actual cyber defense and response to incidents.

Some of these key focus areas include:

### *Incident Classification*

There should exist a well-understood, pre-defined methodology for classifying cyber incidents, especially those that are ultimately defined as material. A clear lexicon of terms as well as roles and responsibilities for detecting and making key decisions on a timely basis will be fundamental.

### *Incident Response*

There should exist a well-structured and efficient process for managing the remediation and recovery of any incident, regardless of materiality. This will include clear identification of roles such as Incident Commander and other key technical support roles.

### *Crisis Response Plans*

The capabilities for managing external communications need to be well-estab-

lished in advance and it is important that this exist as a separate, specialized capability in the communications organization. This is often mistakenly presumed to be included as part of an Incident Response Process, which is more appropriately a technology and operations role with different functions and skills needed for communication with media, regulators, and shareholders.

### *Regular Testing*

Given the necessity for swift materiality assessments and disclosures, operational efficiency is key. Regular drills and simulations, complemented by post-action analyses, can be instrumental in refining processes and roles, ensuring everyone is aligned and any gaps are promptly addressed.

## Critical Infrastructure Considerations

The SEC's new cybersecurity rules are designed to enhance investor understanding and trust regarding cyber risk. More specific and frequent disclosures will likely advance this aim significantly, while at the same time creating several key challenges that operators of critical infrastructure will need to grapple with:

### *Pay Now or Pay Later*

Additional demands on already-strapped experts could be material in companies who are relatively low in their cyber risk management maturities. It will be important to recognize the incremental demands on those resources and budget accordingly with appropriate staffing and enabling technologies. Adopting the new requirements won't "just happen"—specific accountabilities and priorities need to be defined and funded.

### *Regulator Bingo*

The SEC is one of many key regulators that the cyber risk program must account for. In parallel with the SEC reporting requirements, the Cybersecurity & Infrastructure Security Agency (CISA) is finalizing its own incident reporting requirements that will likely be more technical and detailed in nature. Both will seek information on the most relevant, "material" incidents and companies will need to ensure which—or both—regulator requires reporting on which incidents. Key sectors like the electricity industry are already intimately familiar with NERC-CIP requirements that must simultaneously be addressed—and that is just in the United States—similar regulators exist in many other key geographies. Companies need to have an integrated, holistic strategy for harmonizing and synchronizing all these existing regulatory requirements and start building capacity for the inevitable addition of others.

### *Materiality Beyond First-Party*

In addition to the traditional litmus test of materiality as it affects a company's shareholders, critical infrastructure companies can have material impact on stakeholders beyond shareholders. Imagine energy refineries that suffer a hack to industrial control systems that result in physical damage of assets and the release of toxic chemicals, explosions, or fires. Traditional first-party risk management processes will account for the materiality of such incidents to shareholders, the knock-on effect to adjacent communities and the broader commercial ecosystem will also need to be planned for and managed.

## Author Capsule Bio

**Brian Walker** is Founder of the CAP Group, based in Dallas, Texas. The firm pro-vides cyber risk advice to directors and officers of clients ranging in size from global Fortune 500 to regional G2000. He is a frequent writer and speaker on cyber risk strategy—regularly appearing at NACD, PDA, GARP, and others. He has spe-cialized in the formulation of strategies to mature defensive capabilities for criti-cal infrastructure, including both information technology (IT) and operational technology (OT) / industrial control systems (ICS). His assignments have in-cluded global clients, as well as regional clients in North America, Japan, Europe, and Asia. He has led maturation-in-place initiatives as well as provided interim CIO/CISO roles in support of turnaround/urgent situations. He has managed the launch of information security and privacy subcommittees (ISPS), including definition of policy frameworks and all associated policies and standards. Opera-tional responsibilities have included adherence to regulators including SEC, FIN-RA, OCC, NERC, FERC, TSA and DHS. In addition, he has created and matured technology partner ecosystems including cybersecurity, infrastructure operations, cloud services, applications management, and bundled As-A-Service capabilities.