

Foreword by David Hirsch, Former Chief of the Cybersecurity and
Cyber Unit (CACU) within the SEC's Division of Enforcement,
Partner at McGuireWoods

CYBERFIDUCIARY

Navigating SEC Mandates
for Cybersecurity

CRISTINA
DOLAN

SETH JAMES
NIELSON

DOLAN | NIELSON

CYBERFIDUCIARY

BEP

Cyberfiduciary

Navigating SEC Mandates for Cybersecurity

Cristina Dolan and Seth James Nielson



Cyberfiduciary: Navigating SEC Mandates for Cybersecurity

Copyright © Business Expert Press, LLC, 2026.

Cover design by Cristina Dolan and Seth James Nielson

Interior design by S4Carlisle Publishing Services, Chennai, India

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopy, recording, or any other except for brief quotations, not to exceed 400 words, without the prior permission of the publisher.

First published in 2026 by
Business Expert Press, LLC
222 East 46th Street, New York, NY 10017
www.businessexpertpress.com

ISBN-13: 978-1-60649-648-0 (paperback)

ISBN-13: 978-1-60649-649-7 (e-book)

Corporate Governance Collection

First edition: 2026

10 9 8 7 6 5 4 3 2 1

EU SAFETY REPRESENTATIVE

Mare Nostrum Group B.V.

Doelen 72

4831 GR Breda

The Netherlands

gpsr@mare-nostrum.co.uk

CHAPTER 1

The SEC Cybersecurity Disclosure Rules

An Executive Summary of the New Requirements

In July 2023, the SEC adopted groundbreaking rules mandating how public companies must disclose cybersecurity incidents and risk management practices. These rules, taking effect in late 2023 and 2024, create two main obligations:

1. Prompt reporting of material cybersecurity incidents on Form 8-K within four business days of determining materiality (Figure 1.1).
2. Detailed annual disclosures of the firm's cybersecurity risk management, strategy, and governance in Form 10-K.

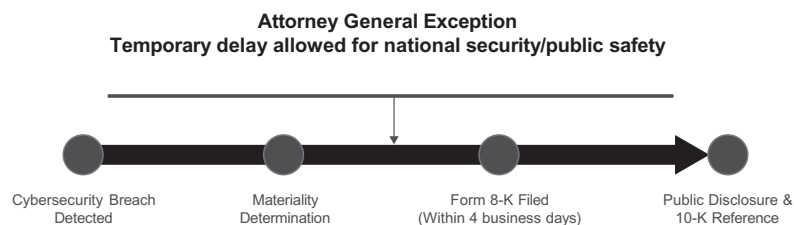


Figure 1.1 *Cybersecurity incident disclosure timeline under the SEC's requirements including internal materiality assessment*

The SEC's goal is to standardize and elevate the information investors receive about companies' cyber risk oversight (Figure 1.2). Notably, the rules also require companies to disclose the board of directors' oversight of cyber risks and whether any board members have cybersecurity

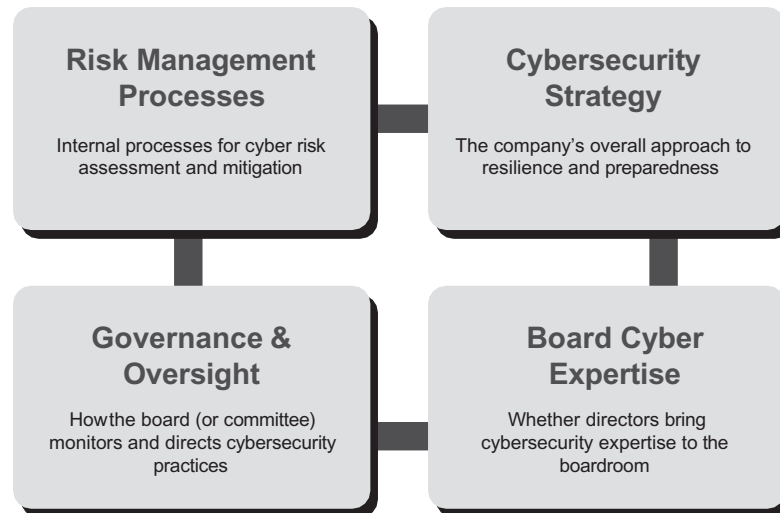


Figure 1.2 Key elements of the SEC-mandated Form 10-K cybersecurity disclosure

expertise. This marks the first time board-level cybersecurity accountability has been explicitly mandated in U.S. securities law, analogous to how Sarbanes–Oxley elevated board oversight of financial reporting.

Many observers have drawn parallels between these cyber disclosure rules and past SEC initiatives for financial transparency. Indeed, we explicitly argue that these new rules are “*Sarbanes–Oxley for cybersecurity*,” given their sweeping scope and emphasis on executive accountability. Like SOX’s Section 302/404 requirements for management certification and internal controls, the SEC’s cyber rules effectively force management to assess and disclose their internal cyber controls annually—a self-assessment that lays the groundwork for future attestation requirements. SEC Chair Gary Gensler analogized cyber incidents to other material business events: “*Whether a company loses a factory in a fire or millions of files in a cybersecurity incident—it may be material to investors.*” In short, cybersecurity is now viewed as a core disclosure issue, much like financial performance, and companies must be as transparent about cyber incidents and preparedness as they are about quarterly earnings. The new role for public boards is that of the Cyberfiduciary.

Key Elements of the SEC's Cyber Disclosure Rules

The rules can be summarized in two parts.

First, Material Incident Reporting

Any “material cybersecurity incident” must be disclosed via an Item 1.05 Form 8-K within four business days after management determines the incident is material. Materiality is defined by the usual standard (information important to the average investor’s decision). In practice, this means companies need internal escalation processes to investigate breaches quickly and decide on materiality “without unreasonable delay.” There is a narrow national security/public safety exception allowing the U.S. Attorney General to temporarily delay disclosure, but otherwise companies cannot defer or obscure a material breach report. Importantly, the SEC does not permit withholding key details out of concern that disclosure might aid attackers or embarrass the company—there is “*no security through obscurity*” defense for omitting facts. Companies must reveal the nature and scope of the incident, when it was discovered, and its material impact or likely impact on finances and operations.

Second, Annual Reporting Requirements

The rules introduce annual reporting requirements (Regulation S-K Item 106) on cybersecurity risk management, strategy, and governance. In each annual 10-K filing, companies must describe: their processes for assessing and managing cyber risks; the material effects of cyber threats and past incidents on the business; the board’s oversight of cyber risks; and management’s role and expertise in handling cybersecurity (including whether they have a designated cyber expert or committee). This effectively forces boards to be actively involved and informed. As one governance advisory firm noted, there was a “*significant increase in disclosure*” about boards’ approaches to cybersecurity once the rules came out. Companies now often formalize cyber oversight responsibility at the board or committee level (indeed, about 74 percent of Russell 3,000 companies have updated

charters to codify cyber oversight). The SEC’s expectation is that directors understand and regularly discuss cybersecurity as part of enterprise risk management (ERM).

A Turning Point for Cyber Governance

The year 2024 thus stands as a turning point in corporate governance: Cybersecurity oversight has been elevated to a top-tier board responsibility, subject to regulatory scrutiny akin to financial reporting post-SOX. Just as SOX brought personal accountability for CEOs/CFOs (certifications) and required robust internal control systems, the SEC’s cyber rules seek to hold senior management and boards accountable for cyber disclosures and preparedness, forcing them to become Cyberfiduciaries. Companies will likely need to implement new internal processes (e.g., disclosure committees for cyber incidents, enhanced IT controls reviews) to ensure they can make the required filings accurately and on time. Failure to do so could expose them to SEC enforcement or shareholder lawsuits for material misstatements. Already, legal analysts point out that these requirements “*increase the risk of litigation over misstatements relating to cybersecurity*” if companies are not diligent (Figure 1.3).

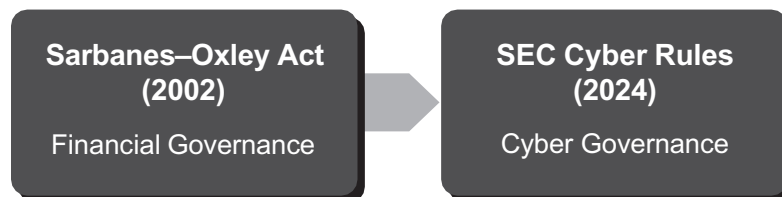


Figure 1.3 Regulatory evolution: from Sarbanes-Oxley (2002) to SEC cyber rules (2024)

KEY TAKEAWAY

Board members of public companies are now responsible for oversight of their companies’ cybersecurity posture and risk management. As with all oversight requirements, this responsibility carries with it the risk of personal litigation if not handled correctly.

While the SEC rules do not dictate specific cybersecurity controls (they are disclosure-based, not prescriptive), they are driving companies to bolster their actual cyber programs. The act of preparing the disclosures forces an internal review of cyber risk management—much as SOX 404’s management assessment did for financial controls. In practice, many companies are choosing to enhance their cyber defenses and governance now, so that they have a positive story to disclose. In fact, regulators have indicated that demonstrating a good-faith effort in cyber governance could influence enforcement: If a breach happens but the company can show it was diligent and had strong controls, the SEC may exercise leniency, whereas negligence or lack of effort will be penalized. This philosophy mirrors the post-SOX enforcement environment, where having a compliance framework and promptly addressing issues can stave off fraud charges.

Cybersecurity has graduated from an “IT issue” to a boardroom issue, with the SEC’s 2023 rules as the catalyst. Executives and directors must approach cyber risks with the same rigor and transparency as financial reporting. The regulatory landscape is evolving quickly—and companies that treat cybersecurity governance as seriously as SOX compliance will be best positioned to meet these new obligations and avoid liability.

Key Requirements of the 2024 SEC Rules

Every public issuer now has two major obligations regarding cybersecurity disclosure:

Report material cyber incidents within four business days

If a company determines that a cybersecurity incident (e.g., a data breach or systems outage caused by a cyberattack) is material to investors, it must file an Item 1.05 Form 8-K disclosure within four business days of that materiality determination. “Material” generally means the incident is significant enough that an investor would consider it important (this could be due to financial impact, operational disruption, or legal implications). The 8-K should describe the nature of the incident, its timing, and its assessed impact. Notably, companies aren’t required to disclose technical details that could further compromise security (and there is a

limited provision for delay if disclosure poses a substantial national security or public safety risk), but the bar for delay is high. In practice, this rule pressures management to swiftly assess incidents and involves the board in deciding what constitutes a material event. It's analogous to how a sudden CFO departure or a significant lawsuit would trigger an 8-K—now a major cyber incident does too, with the same urgency.

Disclose annual cyber risk management and governance practices

In annual reports (Form 10-K for U.S. companies, 20-F for foreign issuers), companies must describe in detail what they are doing about cybersecurity at the governance and management level. This includes explaining the company's processes for assessing and managing cyber risks, and crucially, describing the board of directors' oversight of cybersecurity. For example, the report should state whether the board or a board committee is responsible for cyber oversight, how often cybersecurity is discussed in meetings, and any policies or strategies that inform the board's oversight role. Management's role must also be outlined—for example, is there a CISO reporting to an executive team member, does the company have an internal Cybersecurity Risk Committee, and so on. Essentially, investors should get a clear picture of how seriously the company takes cybersecurity and how responsibilities are allocated from top to bottom. This requirement has the effect of forcing boards to formalize their approach: If a company cannot describe its cyber governance, that is itself a red flag. Many companies have already responded by elevating cybersecurity in board agendas or even adding directors with cyber expertise, so they have a good story to tell in the 10-K.

These two requirements were first proposed by the SEC in 2022 and finalized in July 2023, reflecting a growing consensus that cybersecurity information is material to markets. High-profile incidents like the SolarWinds supply chain attack and the Equifax breach have shown that cyber lapses can erase billions in market cap overnight. Regulators, therefore, want transparency to ensure investors aren't kept in the dark. From the board's perspective, the rules effectively mandate active engagement: Management will be coming to the board with incident assessments (to decide if an 8-K is needed) and with an annual report draft that describes the board's own actions. It's a strong incentive for directors to get educated and involved so they can oversee these disclosures properly.

Materiality and Timing—A Closer Look

One of the trickiest aspects for companies is determining what counts as a “material” incident and when that determination is made. The SEC did not set a dollar threshold; materiality remains the classic judgment call about what a reasonable investor would consider important. Honestly, this is one of the most challenging aspects of the SEC’s requirements because there are no clear bright lines. ***Each organization will have to develop their own guidelines around what is and is not material.*** Obviously, this is an important area for board oversight. The following concepts can help you in this process.

For cybersecurity “materiality,” some good guidelines could include any or all of the following:

- Incidents that incur a financial loss above an established threshold
- Incidents that expose a significant amount of customer data, or incidents that disrupt operations (e.g., a ransomware that halts production), even if the immediate financial cost is modest
- Incidents that expose ***any*** customer data that has regulatory requirements for disclosure
- Incidents that will impact reputation and may influence investor perception
- Incidents that may cause significant outages or downtime, especially if they will be apparent to customers or the public at large
- Incidents that, if somehow not affecting the breached organization, affect customers, suppliers, vendors, or other partners in a material way

Please note that these are guidelines and not legal or regulatory advice. Also note that it does not include specific numbers because those vary from industry to industry and by company size. We take the position that if you are in doubt, you should disclose so however your organization formulates the thresholds, they should err toward the side of disclosure. Moreover, you can also ask yourself the question: How significantly would this disclosure influence investors? If it is likely to influence them, it is probably “material.”

Each organization should define their internal guidelines and policies for materiality determination and disclosures. And the process needs to be efficient and tested. The clock for the four-day 8-K starts ticking once the company determines the incident is material, not from when the incident first occurred. This means companies need internal escalation processes so that cyber incidents are evaluated quickly by the right people (often a management committee, with board notification). If it takes weeks to realize an incident was big enough to be material, the delay could be seen as a failure of internal control.

The board should ensure that management has clear criteria and a response plan for material cyber incidents ahead of time. For instance, applying the guidelines above has led many firms in adopting an internal policy that any breach impacting, say, more than 100,000 customer records or causing over \$X in damages (or X percentage) triggers an immediate briefing to the CEO, General Counsel, and possibly board chair, to decide on disclosure. This kind of preplanning is analogous to having a disaster recovery plan—now it's a disclosure recovery plan (Figure 1.4).

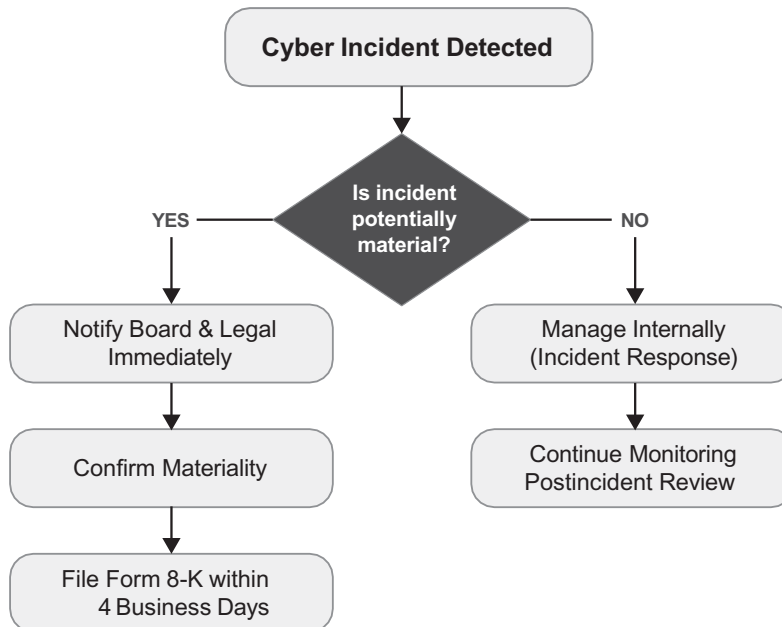


Figure 1.4 Decision framework for determining materiality of cybersecurity incidents

Comparison to Sarbanes–Oxley

While cybersecurity and financial reporting are different domains, the spirit of the SEC’s approach mirrors Sarbanes–Oxley in some ways. One parallel is the emphasis on internal controls. Under SOX Section 404, management must assess and report on the effectiveness of internal controls over financial reporting, and external auditors often attest to it. In the cyber context, there’s no formal requirement for a controls attestation (yet), but by requiring disclosure of risk management processes, the SEC is nudging companies toward establishing robust internal cyber controls and possibly getting third-party assurance (like SOC for Cybersecurity reports) to back up their statements. Another parallel is board expertise and committee structure. SOX led to the rise of Audit Committees with financial experts; the cyber rule has prompted discussions about cyber expertise in the boardroom. As noted, the final rule didn’t mandate an expert, but investors and regulators clearly expect boards to beef up knowledge. The SEC’s Cyber Unit Chief has signaled that they will be looking not just at the fact of a breach but also at how the company’s governance either prevented or failed to prevent it. This is reminiscent of how, post-SOX, regulators started scrutinizing Audit Committee minutes and internal audit reports when investigating financial fraud. Boards should be prepared for the idea that, if a major breach happens, the SEC might ask: What were you, the board, doing on cyber oversight prior to this incident? Knowing that, it’s wise to have a good answer (and documentation to prove it).

A real-world example that underscores the stakes for public companies took place in March 2023. The SEC charged software company Blackbaud, Inc. for failing to fully disclose the scope of a ransomware attack. Blackbaud agreed to pay a \$3 million penalty for its misleading statements. In that case, internal personnel knew more about the breach’s impact than what was conveyed in filings, and the company’s lack of proper disclosure controls caused material facts to be omitted. The SEC’s message was clear—cyber incidents must be reported accurately and promptly, or companies will face consequences. This enforcement action foreshadowed the SEC’s broader policy shift: Soon after, the new disclosure rules were approved, making timely cyber reporting a formal requirement for all public companies (Figure 1.5).

	Sarbanes–Oxley (2002)	SEC Cyber Rules (2024)
Executive Accountability	CEO/CFO Certification of financial statements	CEO/CISO/Board responsibility for cyber disclosures
Board Oversight	Audit Committee Independence and oversight of auditors	Board oversight of cyber risk governance
Disclosure Requirements	Form 10-K/10-Q financial reporting requirements	Form 8-K for incidents, 10-K for annual disclosures
Attestation & Controls	Internal Controls testing (404)	Evidence of cyber risk management & attestation
Penalties for Noncompliance	Civil & criminal penalties for false certifications	Fines, enforcement actions, reputational damage

Figure 1.5 Regulatory evolution of SEC Cyber Rules mirror the Sarbanes-Oxley framework for financial governance

KEY TAKEAWAY

Because cybersecurity reporting requirements are part of SEC disclosure rules, public boards have responsibilities to ensure that public disclosures materially reflect the underlying realities.

Summary

The SEC’s 2024 cybersecurity disclosure rules have formalized what leading practitioners have long advised: Cyber risk is enterprise risk and must be governed with transparency and rigor. For boards and executives, compliance will require a combination of prompt incident response protocols, thorough governance disclosures, and continuous oversight improvements in order for them to effectively operate as Cyberfiduciaries. The following chapters will build on this foundation. Next, we will examine how exactly a board should organize itself to meet these expectations (“noses in, fingers out” in action), and later, how to generate the evidence (attestations, reports, training records) that demonstrate your compliance in case regulators or litigants come knocking.

About the Authors



Cristina Dolan is a veteran technology executive and public company board director known for driving digital innovation and strong governance. She has extensive leadership experience at the intersection of technology, cybersecurity, AI, and fintech. Ms. Dolan cofounded OneMain.com, serving as division president and leading it through a NASDAQ IPO and subsequent acquisition. She has since held multiple public company board roles: cur-

rently as a non-executive director and audit committee chair of SEALSQ (NASDAQ: LAES), and formerly as a director on the boards of WiseKey (NASDAQ: WKEY) and GRIID (NASDAQ: GRDI, acquired by Cleanspark), where she also served on special committees and oversaw audit and compensation governance. In these roles, Ms. Dolan has been deeply involved in overseeing cybersecurity risk disclosures and compliance with U.S. and global regulations. As an executive adviser at Crimson Vista, Inc., she has contributed her boardroom perspective to cybersecurity audit and attestation services for clients. In addition to holding executive roles at RSA Netwitness, Disney, Hearst, IBM, and Oracle, she served as CEO of a venture-based AI company spun out of MIT. The best-selling sustainability book she co-authored, *Transparency in ESG and the Circular Economy: Capturing Opportunities Through Data*, has received international recognition. Additionally, Ms. Dolan is an adjunct professor at Columbia University's Technology Management program, educating future leaders on cybersecurity, risk management, Industry 5.0 technologies, and design thinking methodologies. The MIT Media Lab has named her a Cybersecurity Fellow in its sAlpien program. Her background combining entrepreneurial success, board governance in tech-driven

companies, and academic insight provides a rich perspective throughout this book. She leverages firsthand knowledge of fiduciary duties and regulatory expectations to help boards and executives develop effective oversight of cybersecurity, ESG, AI, and emerging technology risks. Cristina earned a master's degree from the MIT Media Lab and holds a master of computer science engineering and bachelor of electrical engineering.



Seth James Nielson is a subject-matter expert in cybersecurity, software engineering, and computer networks. In his 25-year career, he has worked in academia, industry, research, design, engineering, litigation consulting, and government advising. He earned a BS and MS in Computer Science from Brigham Young University and a PhD

in Computer Science from Rice University. Dr. Nielson is the CEO of Crimson Vista, where he leads forensic investigations, specialized security services, cybersecurity audits, compliance assessments, and strategic advisory services for public companies and government agencies. He also serves as an adjunct faculty member at the University of Texas at Austin, having taught undergraduate cybersecurity and special classes on cybersecurity in practice. Dr. Nielson has consulted on a wide range of technical projects, including secure communications systems, hardware-based cryptography acceleration, secure file storage architectures, privacy enhancing technologies, and vulnerability analysis. He has been retained by organizations from startups to Fortune 100 companies to evaluate security postures and advise on cyber defense strategies. He also investigates cryptocurrency theft and data forensics matters. In addition to technical consulting, Dr. Nielson has served as an expert witness in numerous legal cases involving cybersecurity issues, providing testimony and reports in litigation related to matters such as high-frequency trading algorithms, antivirus efficacy, firewall design, e-commerce encryption protocols, and ransomware impacts. This blend of deep technical expertise and practical experience with compliance and legal accountability uniquely positions him to guide corporate leaders through complex cyber governance challenges.