CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 4, No. 1
April 2025
ISSN: 2832-1006

In this issue:

4. **Education Impact on Trust in Election Technology & Security: Research Proposal**
Garry White, Texas State University
Ju Long, Texas State University

13. **Cybersecurity Apprenticeships: Case-Study of a Four-Year Youth Apprenticeship Program**
Paul Wagner, University of Arizona
Cathleen Barton, Cathleen Barton Consulting

24. ***Teaching Case***
Reshaping Cybersecurity Ethics Education: Evaluating a Posthumanist Pedagogy Using Human/AI Co-Generated Case Studies
Ryan Straight, University of Arizona
Jonathan Lowery, University of Arizona
David Poehlman, University of Arizona
Waamene Yowika, University of Arizona

35. **A Pivotal Progression of SEC's Cybersecurity Disclosure Requirements**
Yining Chen, Western Kentucky University
Divine Lokuku, Western Kentucky University
Tong Wu, Western Kentucky University

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2025 ISCAP Board of Directors

Amy Connolly James Madison University President	Michael Smith Georgia Institute of Technology Vice President	Jeff Cummings Univ of NC Wilmington Past President
David Firth University of Montana Director	Mark Frydenberg Bentley University Director/Secretary	David Gomillion Texas A&M University Director
Leigh Mutchler James Madison University Director	RJ Podeschi Millikin University Director/Treasurer	Jeffry Babb West Texas A&M University Director/Curricular Matters
Eric Breimer Siena College Director/2024 Conf Chair	Tom Janicki Univ of NC Wilmington Director/Meeting Planner	Xihui "Paul" Zhang University of North Alabama Director/JISE Editor

Copyright ©2025 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to editorcppj@iscap.us.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

Anthony Serapiglia
Co-Editor
Saint Vincent College

Jeffrey Cummings
Co-Editor
University of North Carolina Wilmington

Thomas Janicki
Publisher
University of North Carolina Wilmington

2025 Review Board

Cheryl Beauchamp
Regent University

Ulku Clark
Univ of NC Wilmington

Peter Draus
Robert Morris University

Nick Giacobe
Penn State University

Mike Hills
Penn State University

Jeff Landry
Univ of South Alabama

Li-Jen Lester
Sam Houston State Univ

Jim Marquardson
Robert Morris University

Stan Mierzwa
Kean University

Etezady Nooredin
University of New Mexico

Ron Pike
Cal Poly Pomona

RJ Podeschi
Milliken University

Samuel Sambasivam
Woodbury University

Kevin Slonka
Saint Francis University

Geoff Stoker
Univ of NC Wilmington

Paul Wagner
University of Arizona

Ping Wang
Robert Morris University

Tobi West
Coastline College

Johnathan Yerby
Mercer University

A Pivotal Progression of SEC's Cybersecurity Disclosure Requirements

Yining Chen
yining.chen@wku.edu

Divine Lokuku
lokukud@gmail.com

Tong Wu
tong.wu@wku.edu

Western Kentucky University
Bowling Green, KY 42101

Abstract

The U.S. Securities and Exchange Commission (SEC) introduced rigorous cybersecurity disclosure regulation mandating public companies to make prompt disclosure of material cybersecurity incidents and annual disclosure for cybersecurity risk management, strategy, and governance. The SEC's important progression of cybersecurity disclosure requirements signifies forward movement on ensuring transparency and maintaining investor confidence and market integrity. This study reviews the provisions of the new SEC cybersecurity disclosure rules and their implications for corporate governance, investor confidence, and the broader financial ecosystem. The information we present provides educators with pedagogical resources and teaching aids. To assist SEC registrants in adopting and complying with the new rules, we discuss implementation challenges and offer normative suggestions.

Keywords: cybersecurity disclosure, SEC rules, information asymmetry, materiality, transparency

Recommended Citation: Chen, Y., Lokuku, D., Wu, T., (2024). A Pivotal Progression of SEC's Cybersecurity Disclosure Requirements. *Cybersecurity Pedagogy and Practice Journal.* v4, n1, pp 35-44. DOI# https://doi.org/10.62273/MMYQ9950

©2025 ISCAP (Information Systems and Computing Academic Professionals)

A Pivotal Progression of SEC's Cybersecurity Disclosure Requirements

Yining Chen, Divine Lokuku and Tong Wu

1. INTRODUCTION

The digital age has ushered in unprecedented business opportunities, but it has also uncovered a new domain of challenges in the form of cyberattacks (Burt, 2023). The escalating frequency and severity of cyberattacks have necessitated a reevaluation of regulatory policies related to cybersecurity. The SEC's historical guidance on cybersecurity disclosures has been broad, affording companies significant discretion. However, the evolving threat landscape has prompted the SEC to adopt a more proactive stance, necessitating a reexamination and reinforcement of cybersecurity disclosure requirements (Vander & Rotman, 2024).

To address the evolving threat landscape posed by cyberattacks, the SEC implemented final rules, effective December 18, 2023, requiring public companies to disclose material cybersecurity incidents in their quarterly report on Form 8-K within four business days of the incident being determined material. Additionally, detailed information about cybersecurity risk management, strategy, and governance must be disclosed annually on Form 10-K.

In its press release, the SEC highlighted pivotal information regarding the recently adopted cybersecurity disclosure requirements. According to the press release, registrants are "to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance" (Securities and Exchange Commission, 2023a, para. 1). Notably, the new disclosure rules are applicable to not just malicious cyberattacks. Accidental occurrences not caused by a malicious attack, e.g., material internal systems failure, are also in the domain of the new rules. Besides, Form 8-K disclosure requirements are applicable when a company is materially affected by a series of related incidents, even if each individual incident is immaterial. What is more, the Commission has adopted rules requiring foreign private issuers to make comparable disclosures (Securities and Exchange Commission, 2023a).

Form 8-K Item 1.05 – Incident Disclosure

The new Item 1.05 of Form 8-K requires registrants to make timely disclosures of material cybersecurity incidents. Information disclosed, as illustrated in Figure 1, includes:

- Description — nature (e.g., unauthorized access, data breach, or system compromise), timing, and scope of the incident and its financial, operational, and reputational impact.
- Impact — material impact, reasonably likely material impact, and unknown but likely material impact of the incident on the registrant.
- Response — actions taken or undergoing to remediate the incident such as stringency containment measures or changes to policies and procedures.

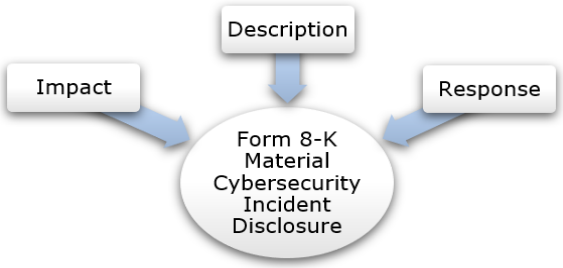


Figure 1: Form 8-K Incident Disclosure

Note: This figure shows the required Form 8-K disclosure for material cybersecurity incidents. The source of information for this figure is the Securities and Exchange Commission (2023a), SEC Press Release, 2023-139.

Form 10-K – Annual Disclosure

Form 10-K Item 106(b) requires registrants to make annual disclosures related to cybersecurity risk management, strategy, and governance. The annual cybersecurity disclosure must be included in the registrant's annual reports for fiscal years ending on or after December 15, 2023. Information disclosed, as illustrated in Figure 2, includes:

- Cybersecurity landscape, investments, and enhancement programs,

- Cybersecurity threats and previous incidents that have materially affected or are reasonably likely to materially affect the registrant, including their likelihood, severity, and impacts on business strategy, operations, or financial condition,
- Cybersecurity risk strategies and management, integrated into the registrant's risk management system or performed by third-party service providers, to identify, assess, and manage material cybersecurity threats, and
  Cybersecurity governance and oversight by board, management, and executives.

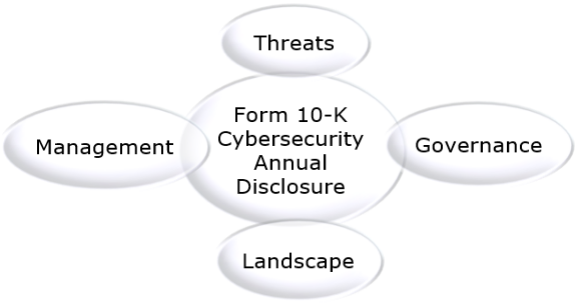


Figure 2: Form 10-K Annual Disclosure

Note: This figure shows the required information for the Form 10-K annual cybersecurity disclosures. The source of information for this figure is the Securities and Exchange Commission (2023a), SEC Press Release, 2023-139.

On Form 10-K Item 106(c)(2), registrant discloses how management assesses and responds to material cybersecurity threats, including, but not limited to (1) which management positions or committees are responsible for assessing and managing cybersecurity risks, and their relevant expertise (2) the processes by which such persons or committees monitor cybersecurity incidents, and (3) how management reports cybersecurity information to the board of directors and its cybersecurity committee. On Form 10-K Item 106(c)(1), registrant provides details for the governance and oversight of cybersecurity risk, including (1) the board's oversight of cyber risks and threats, (2) the board committee or subcommittee responsible for oversight, and (3) the processes by which the board or its committee is informed of cyber risks and attacks (Mazor et al., 2023).

2. KEY PROVISIONS

The new SEC cybersecurity disclosure requirements mark a notable departure from the previous laissez-faire approach, ushering in a more stringent and targeted set of guidelines for companies to adhere to. The provisions of these new requirements include the following.

Timely Disclosure
The SEC mandates companies to promptly disclose cybersecurity incidents, ensuring that investors receive timely and accurate information about potential risks. However, challenges arise from the stringency of the deadlines imposed and more so for specific industries and business styles. The new SEC regulations primarily require companies to disclose material cyberattacks within four days of becoming aware of the issue (Black et al., 2023). Notably, this four-day deadline is, as a rule, applicable across all businesses, though distinct and more stringent deadlines exist for specific industries. For instance, Critical Infrastructure Operators are obligated to report attacks within a tighter timeframe of 72 hours. Investment funds and advisors face an even more accelerated reporting requirement, needing to report incidents within 48 hours (Ciampa, 2023).

Materiality Assessment
The new cybersecurity disclosure requirements place significant emphasis on conducting a comprehensive materiality assessment to determine the significance of a cybersecurity incident. This assessment extends to evaluating the potential impact on the company's operations, financial condition, and reputation. However, it is crucial to note an exception to this rule: companies are not compelled to disclose "specific or technical information about their planned responses to the incident" (Black et al., 2023, para. 9).

Risk Factors
Companies are now obligated to furnish detailed information regarding the specific risks they encounter due to cybersecurity threats. This encompasses disclosing potential vulnerabilities, the likelihood of a cybersecurity incident occurring, and the potential magnitude of its impact. Importantly, this information is required to be reported annually on Form 10-K, as stipulated by the U.S. Securities and Exchange Commission.

Incident Response and Mitigation
The new cybersecurity disclosure requirements mandate companies to disclose their incident response and mitigation strategies comprehensively. This encompasses detailing the specific measures taken to address the incident, prevent future occurrences, and the potential costs associated with remediation efforts.

3. BACKGROUND AND LITERATURE

Cybersecurity Threats

A cyberattack is an intentional and malicious effort to breach the systems of another organization or individual (IBM, 2024). The attacker's motives may be information theft, financial gain, espionage, or sabotage. The SEC defines a cybersecurity incident as "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a company's information systems that jeopardizes the confidentiality, integrity, or availability of the company's information systems or any information residing therein" (Black et al., 2023, para.6).

The increase in cyberattacks and cybersecurity risks is an undesirable outcome of modern business models and tech platforms such as e-commerce, remote work, digital payments, crypto assets, AI, and cloud computing, among others. While advanced technologies make business opportunities possible as never before, the unforeseen effects coming along are unprecedented cybersecurity threats and crises as well as skyrocketing cybercrime costs to companies and investors. Common cyber threats include ransomware, data breaches, stealth malware, underground trends, and AI fraud, while common attacking avenues include business email compromises, targeted cloud services, zero-day exploits, and link library abuse (Lavorgna, 2020).

Rising with the complexity and frequency of cyber threats is the ramping up of regulatory efforts. The SEC has undertaken several initiatives to issue guidance on cybersecurity risk and incident disclosures. Specifically, in 2011, the SEC staff issued guidance, and later in 2018, issued Commission Statement and Guidance on Public Company Cybersecurity Disclosures to help registrants prepare cybersecurity risk and incident disclosures (Gerding, 2023) and to promote clear and vigorous disclosures about cybersecurity, the risk factors, and incidents (Peng & Krivacek, 2020). Even with considerable effort, the Commission admitted that disclosure practices remain inconsistent.

Cereola & Dynowska (2019, "Abstract" section) denote that "although the SEC staff guidance warns public companies to make timely disclosure, recognizing the threat that cybercrime poses to investors in the public markets, it does not go far enough to institute direct measures that would compel companies to reveal the nature and scope of a cybersecurity breach." Their empirical findings indicate a sizable increase "in the number of firms referencing cybersecurity in the Risk Factor section of the 10-K." However, "there is a tendency not to disclose reported breaches in the narrative of the 10-K and that the cybersecurity risk factor disclosures do not include details on actual breaches."

The Commission's recent ruling represents its efforts "to provide investors with the more timely, consistent, comparable, and decision-useful information they need to make informed investment and voting decisions" (Gerding, 2023, para. 2).

Disclosure and Transparency

While disclosure regulations, in general, are expected to improve the quality of reporting and disclosure, the chief benefit reached is the mitigation of information asymmetry and the enhancement of corporate transparency (Bhattacharya et al., 2013). Brown & Martinsson (2018) find that the securities market disclosure reforms foster rich and transparent information environments.

From the existing literature, several empirical studies examine the market impact of mandatory disclosures. For instance, Wang & Fan (2014) explore the impact of R&D disclosure choices (capitalization and expensing) on firm value. Tang et al. (2013) study the capital market reaction to the mandatory disclosure of directors' opinions. Chen et al. (2018) investigate the effect of mandatory CSR disclosure on firm profitability. Xu et al. (2020) examine the effect of CSR disclosure on firm value.

Although high-quality disclosure is proven effective in reducing the information asymmetry between investors and management concerning company performance (Clinch et al., 2012), investors and other financial statement users are usually unable to discern its quality. Edwige & Levine (2020) model an information mosaic theory suggesting that voluntary public disclosures lead to higher *ex ante* information asymmetry by allowing the informed trader to refine his or her trading strategy and complete the information mosaic. Proponents of mandatory disclosure and policymakers argue from a social psychology perspective that disclosing value-relevant information makes firms' accountability more salient, thereby reducing agency costs. With the reduced information asymmetry and agency conflicts, users of financial information can make more informed decisions.

Healy & Palepu (2001, p. 406) argue that the "demand for financial reporting and disclosure arises from information asymmetry and agency conflicts between management and outside investors. The credibility of management disclosures is enhanced by regulators, standard setters, auditors, and other capital market intermediaries." While research finds broad support that disclosure regulation brings about new and relevant information to investors (Kothari, 2001), whether a particular disclosure regulation is effective in alleviating information asymmetry and agency problems remains a research question, especially when new disclosure regulations are enacted. Whether a particular disclosure regulation, such as a mandatory cybersecurity disclosure regulation, is effective in producing positive economic consequences is of greater interest to regulators, standard-setters, firms, and investors.

4. IMPLICATIONS OF THE SEC RULING

Although this study does not provide empirical evidence on the effectiveness of the new SEC cybersecurity disclosure rules, we deliberate on the provisions of the new rules and their implications for corporate governance, investor confidence, and the broader financial ecosystem.

Corporate Governance
The enhanced SEC cybersecurity disclosure requirements have profound implications for corporate governance. Companies are now compelled to elevate cybersecurity risk management to a strategic consideration for boards and executives, reflecting the interconnectedness between cybersecurity and overall corporate performance.

- Board Oversight: The growing recognition of the board's responsibility in ensuring the company's resilience against cyber threats. The board must exercise its oversight function by overseeing the management team's effort in managing cyber risks and responding to material incidents.
- Integration with Enterprise Risk Management: Companies are encouraged to integrate cybersecurity risk into their broader enterprise risk management framework, fostering a holistic approach to risk assessment and mitigation.
- Accountability and Transparency: Increased transparency promotes accountability among corporate leaders, holding executives responsible for ensuring effective cybersecurity measures are in place and transparently communicating the impacts of incidents.
- Evaluation and Control: Clearly defined reporting chain and materiality evaluation mechanism to ensure that cybersecurity risk evaluations and incidents are reported timely (Peng & Krivacek, 2020).

Investor Confidence and Market Integrity
Investor confidence is paramount to the functioning of capital markets. The new cybersecurity disclosure requirements aim to bolster investor confidence by providing more comprehensive and timely information about the risks companies face in the digital era.

- Informed Decision-Making: Investors armed with more detailed and timely information can make informed decisions, aligning with the SEC's mission of protecting investors and maintaining fair and efficient markets.
- Market Integrity: Reduced information asymmetry contributes to market integrity, allowing investors to more accurately assess the true value and risk associated with their investments, thereby enhancing market stability.
- Sector-Wide Impact: The SEC's cybersecurity disclosure requirements catalyze a collective improvement in cybersecurity resilience across industries, benefiting the entire financial ecosystem.

5. CHALLENGES AND CRITICISMS

The SEC's new cybersecurity disclosure requirements signify a positive stride toward ensuring reporting transparency and informed decision-making for both investors and companies. While these disclosure regulations are a commendable initiative, certain limitations, criticisms, and challenges merit consideration.

First, to comply with the new disclosure requirements, companies need to grapple with balancing the need for transparency and the protection of sensitive information. Also, critics argue that smaller companies with limited resources may bear an undue burden because of the cost of dealing with a potentially massive incident relative to company size (Securities and Exchange Commission, 2023b). Another notable concern is the existence of varied reporting deadlines. Last and foremost, the principal deadline, four business days from the date on which the incident is determined material, presents a substantial challenge.

An illustrative example is the cyberattack experienced by Clorox recently. The incident occurred after the implementation of the disclosure requirements, compelling the company to fully disclose the situation promptly. However, due to the pressing four-day reporting deadline, Clorox's initial 8-K report lacked substantial information as the company was still assessing the material impact of the attack. Clorox later filed multiple 8-K forms to update investors on the incident. This situation aligns with the sentiment expressed by an executive of Clorox, stating that "the fog of these incidents will make it hard to provide reliable information at the start" (Nash, 2023, para. 3). As exemplified, the new cybersecurity disclosure requirements are novel for companies, leading many to file Form 8-K without a thorough investigation into the incident's implications for their operations. This dilemma risks information overload and can adversely affect a company's stock value, as displayed in the case of Clorox.

Zukis (2024) examines cybersecurity disclosures that have been filed since the enactment of the SEC cybersecurity disclosure ruling and finds deficiency and noncompliance. Specifically, none of the first filers include quantitative disclosures of the material impacts or reasonably likely material impacts of the incident. The materiality disclosures are all based exclusively on the qualitative impacts of the incident, and none reference quantitative financial impacts due to the common reporting difficulty that "incident costs and financial implications typically lag as the incident plays out" (Zukis, 2024, para. 19).

Another noteworthy concern of implementation is the absence of specificity in determining materiality. The new SEC rules do not explicitly state who should decide materiality. Neither do they provide guidelines on evaluating if an incident should be deemed material. In fact, registrants may not be able to determine the materiality of an incident immediately after its discovery. While the SEC sets a stringent deadline (i.e., four days) to disclose an incident on Form 8-K from the date on which the incident is considered material, it does not set a specific deadline by which a registrant must determine whether an incident is material after its discovery. The only general rule is to make materiality determinations without unreasonable delay (Mazor et al., 2023).

6. MATERIALITY

The SEC defines a material incident as one that a reasonable shareholder would consider important in making an investment decision (Securities and Exchange Commission, 2023a). Specifically, an incident is considered material "if it significantly affects a company's operations, financial positions, reputation, or legal obligations" (Vander & Rotman, 2024, para. 2). This definition of materiality, however, lacks a clear objective threshold and therefore presents challenges for companies to assess cybersecurity incidents or to justify their disclosure decisions to regulatory authorities and interested parties.

The SEC cybersecurity disclosure rules are expected to be updated as more insights emerge. Also, better methodologies will be developed to guide companies in navigating this evolving landscape. But before any additional guidelines become available, it is important for companies to strive for best practices. With precise and timely disclosure of material incidents, companies can preserve trust from interested parties amidst cyber crises and attacks. To do so, companies should develop a clear process with proper mechanisms to determine materiality for cybersecurity incidents. The process should (1) require the IT function to play an integral role, (2) solicit support from legal counsels and financial advisors, (3) account for actual and expected impacts, and (4) consider both qualitative and quantitative factors (Vander & Rotman, 2024).

Quantitative factors that make an actual impact on the assessment of materiality include ransom payments, restoration costs, operational disruptions, earnings and stock price losses, and legal and litigation fees. Other quantitative factors with expected impacts may be costs to repair and strengthen system security and environment and future insurance and protection costs. Besides these actual and expected quantitative factors, qualitative factors to consider include reputation damage, goodwill impairment, supply chain and customer relationship destruction, motivation of malicious invader, and legal disputes and liabilities.

Vander & Rotman (2024) suggest that companies design or adopt a framework for their materiality assessment. The framework should suit the company's functions, leverage a combination of quantitative and qualitative factors, allow individual considerations for different incidents, offer a taxonomy of loss categories, and document the materiality assessment processes and decision points. The framework, like other frameworks used for business continuity and disaster recovery plans, data privacy and security policies, and enterprise risk management

programs, should be subject to continuous evaluation and improvement.

As a final point, when encountering cybersecurity incidents, companies need to assess whether the incident is material from the perspective of stakeholders rather than their own. They need to objectively evaluate whether investors and stakeholders would consider the incident material in making their investment decisions. To ensure the objective assessment of materiality, timely response and reporting of cybersecurity incidents, and proper adherence to the SEC disclosure requirements, companies can form a cross-functional disclosure team consisting of information security officers, risk management personnel, legal counsels, financial advisors, and board representatives (Vander & Rotman, 2024; Johnson, 2024).

7. COMPLIANCE PREPARATION

To implement the SEC cybersecurity disclosure requirements to achieve successful compliance, registrants should take preparation actions. They can build upon the lessons learned from prior compliance initiatives with the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the PCI security standards. Many of these regulations and standards have stricter requirements and their compliance solutions may have a synergistic effect in solving cybersecurity challenges. As cybersecurity challenges escalate and regulations multiply, it is increasingly important that companies develop not only sustainable programs to manage cybersecurity risks but also sensible strategies to comply with regulations and disclosure requirements. We show viable preparation actions in Figure 3, then explain them in the following sections.



Figure 3: Preparation Actions

Note: This figure suggests actions that SEC registrants can take to prepare for the new cybersecurity disclosure requirements. The source of information for this figure includes Mossburg et al. (2023) and Ehret (2023).

Conduct Readiness Assessment

First, registrants should assess their mindset acknowledging that cybersecurity is no longer bolt-on after cyberattacks, but rather baked-in as a core element of organizational culture (Rosone & Kleemann, 2023). Second, registrants should institute a foundation cultivating evolving capabilities in response to evolving threats. They should form a cybersecurity response and reporting team and ensure their mature understanding of the incident response and reporting processes. Third, registrants should prepare for the SEC's effect on the labor market, expecting a shortage of executives with cybersecurity experience and capabilities. They will need to reserve proper executives with talent aligning with the SEC requirements. Fourth, registrants need to assess their reliance on third-party service providers, and whether they have processes to oversee and identify cybersecurity threats associated with their use of third-party services.

Revise Incident Response Policies and Procedures

It's important that registrants revisit cybersecurity policies to ensure that they provide effective disclosure controls and procedures, including communication channels between the cybersecurity team, the investor relations advisor, and the legal counsel. These policies and channels of communication will be the core to the prompt assessment and response to detected cybersecurity incidents as well as the precise and timely compliance with the new disclosure requirements.

Cyber strategies, policies, and procedures must include response and recovery plans and periodic risk assessments. Registrants should test their adequacy and effectiveness and update them on a continuous basis to ensure compliance with applicable regulations and laws. In addition, cyber policies, procedures, and practices should be extended to third-party service providers.

Reinforce Governance and Oversight Structures

To prepare for compliance, registrants should adopt the mindset to provide shareholders and the public with confidence that cybersecurity is a top organizational priority. Their organizational security governance (OSG) practices should allow quick and reliable decision-making and adapt to the changing landscape of security management (Slonka et al., 2023). With the aim of doing this,

registrants should strengthen the cybersecurity governance structure by (1) educating the board and executives, (2) fostering a culture of responsibility and accountability, (3) delegating a specific board committee responsible for supervision, and (4) plotting operating models for cyber risk management and disclosure.

Expand Incident Response and Reporting Capabilities

It is essential that registrants invest in cyber-resilience and expand incident response capabilities. The incident response and reporting system should adopt a materiality framework, define materiality criteria, and form incident assessment processes. The materiality, e.g., complexity and severity, of the cybersecurity risk must be considered from each registrant's business risk, technology, reputation, and regulatory compliance perspective. There is no one-size-fits-all approach (Ehret, 2023). Besides, the system should have the capacity to meet disclosure obligations as incidents evolve and to learn from past incidents to improve resilience. Altogether, the cyber risk response system should promptly identify and address incidents in order to protect the organization against cyber risks and safeguard its reputation. It should facilitate timely and informative incident disclosures as well as consistent and transparent periodic disclosures.

Minimize Cyber Attack Risk and Threats

The best way to prepare for the stricter SEC disclosure rules is to minimize the possibility of data breach and system compromise. For registrants to boost up cyber risk defense, we make a few suggestions. First, invest in in-house or third-party security technologies, such as multi-layer and multi-factor access authentication, to strengthen identity and access controls. Second, secure cloud connection and remote access via enhanced network protection and intrusion detection systems. Third, perform penetration testing to identify weak spots in a system's defenses. Fourth, investigate emerging threat actors and their best defense. Fifth, train legal, infosec, and operational teams for breach prevention, response, mitigation, and reporting.

8. CONCLUSION

The SEC's enhanced cybersecurity disclosure requirements mark a pivotal progression in regulatory history, acknowledging cybersecurity as integral in maintaining investor confidence and market integrity. By mandating detailed and timely disclosures, the SEC aims to empower investors' decision-making and incentivize companies to prioritize cybersecurity within their corporate governance frameworks. As businesses navigate the complexities of the digital age, the new regulations offer a roadmap for building resilience and stability of corporate governance and ensuring the long-term sustainability of the financial ecosystem.

As the cybersecurity landscape continues to evolve, the SEC is likely to refine its disclosure requirements to address emerging challenges. Continued emphasis on transparency, accountability, and the integration of cybersecurity risk into corporate governance frameworks is anticipated. As companies move forward on the journey of compliance, disclosure examples will be set and penalties imposed, forcing all organizations into developing comprehensive materiality determination framework and structured reporting processes. (Zukis, 2024). At the other end, investors and stakeholders, with a regulatory baseline now in place, will persist in demanding more and better disclosures on material cybersecurity incidents and on how systems and data are secured, managed, and governed to support company values.

9. REFERENCES

Bhattacharya, N., Hemang, D., & Venkataraman, K. (2013). Does earnings quality affect information asymmetry? Evidence from trading costs, *Contemporary Accounting Research, 30*(2), 482-516. https://doi.org/10.1111/j.1911-3846.2012.01161.x

Black, E. W., Kent, E., & Halbhuber, H. (2023). New SEC cybersecurity disclosures. *The Harvard Law School Forum on Corporate Governance*, August 13. https://corpgov.law.harvard.edu/2023/08/13/new-sec-cybersecurity-disclosures/

Brown, J. R., & Martinsson, G. (2018). Does transparency stifle or facilitate innovation? *Management Science, 65*(4), 1600–1623. https://doi.org/10.1287/mnsc.2017.3002

Burt, A. (2023). The digital world is changing rapidly. Your cybersecurity needs to keep up. *Harvard Business Review*. Retrieved November 27, 2024 from https://hbr.org/2023/05/the-digital-world-is-changing-rapidly-your-cybersecurity-needs-to-keep-up

Cereola, D. J., & Dynowska, J. (2019). Investigating the impact of publicly announced information security breaches on

corporate risk factor disclosure tendencies. *Journal of Cybersecurity Education*, *Research, and Practice, 2019*(2). https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss2/3/

Chen, Y. C., Hung, M., & Wang, Y. (2018). The effect of mandatory CSR disclosure on firm profitability and social externalities: Evidence from China. *Journal of Accounting and Economics, 65*(1), 169-190. https://doi.org/10.1016/j.jacceco.2017.11.009

Ciampa, M. (2023). Too much disclosure? Or not enough? Working Paper. Western Kentucky University.

Clinch, G., Stokes, D. J., & Zhu, T. (2012). Audit quality and information asymmetry between traders. *Accounting and Finance, 52*(3), 743-765. https://doi.org/10.1111/ j.1467-629X.2011.00411.xEdwige, C., & Levine, C. B. (2020). Public disclosures and information asymmetry: A theory of the mosaic. *The Accounting Review, 95*(1), 79–99. https://doi.org/ 10.2308/accr-52447

Ehret, T. (2023). Companies should prepare to comply with new SEC cybersecurity rules. Thomson Reuters. Retrieved November 28 from https://www. thomsonreuters.com/en-us/posts/ government/sec-cybersecurity-rules/

Gerding, E. (2023). Cybersecurity disclosure. SEC Statement, Dec. 14. https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214

Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics, 31*(1-3), 405-440. https://doi. org/10.1016/S0165-4101(01)00018-0

IBM (2024). What is a cyberattack? Retrieved November 20, 2024 from https://www.ibm.com/topics/cyber-attack#:~:text=A%20cyberattack%20is%20any%20intentional,theft%20to%20acts%20of%20war

Johnson, M. (2024). Why new SEC cybersecurity rules require an integrated approach, EY. https://www.ey.com/en_us/ cybersecurity/new-sec-cybersecurity-rules-require-integrated-approach

Kothari, S. P. (2001). Capital markets research in accounting. *Journal of Accounting and Economics 31*, 105-231. https://doi.org/10.1016/S0165-4101(01)00030-1

Lavorgna, A. (2020). *Cybercrimes: Critical issues in a global context*. Bloomsbury Publishing.

Mazor, C., Herrygers, S., & Danola, C. (2023). SEC issues new requirements for cybersecurity disclosures, *Deloitte Heads Up, 30*(13), July 30 (Updated Dec. 19). https://dart.deloitte.com/USDART/home/publications/deloitte/heads-up/2023/sec-rule-cyber-disclosures

Mossburg, E., Amjad, A., Kumar, G., Adib, N., Herrygers, S. & Mazor, C. (2023). Navigating the new SEC cybersecurity disclosure requirements, Deloitte, Retrieved November 28, 2024 from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-navigating-the-new-sec-cybersecurity.pdf

Nash, K. S. (2023). Clorox cyberattack brings early test of new SEC Cyber Rules. *The Wall Street Journal*, September 20. https://www.wsj.com/articles/clorox-cyberattack-brings-early-test-of-new-sec-cyber-rules-b320475

Peng, J., & Krivacek, G. (2020). The Growing Role of Cybersecurity Disclosures. *ISACA Journal*, *1*, February 26, 2020. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/the-growing-role-of-cybersecurity-disclosures

Rosone, B., & Kleemann, T. (2023). What new SEC cyber ruling requirements could mean for private companies. Deloitte Debriefs, November 1. 2023. https://www2.deloitte.com/us/en/events/private-companies-dbriefs-webcasts/2023/new-sec-cyber-ruling-requirements.html

Slonka, K., Mishra, S., Draus, P., & Bromall, N. (2023). Measurement, reporting, and monitoring in organizational security governance from the security professional's perspective. *Cybersecurity Pedagogy and Practice Journal, 2*(1), 38-49. https://cppj.info/2023-2/n1/CPPJv2n1p38.html

Tang, X., Du, J., & Hou, Q. (2013). The effectiveness of the mandatory disclosure of independent directors' opinions: Empirical evidence from China, *Journal of Accounting and Public Policy, 32*(3), 89-125. https://doi.org/10.1002/smj.2421

Securities and Exchange Commission (2023a). SEC adopts rules on cybersecurity risk

management, strategy, governance, and incident disclosure by public companies, SEC Press Release, 2023-139. https://www.sec.gov/news/press-release/2023-139

Securities and Exchange Commission (2023b). Cybersecurity risk management, strategy, governance, and incident disclosure. *Federal Register, 88*(149), August 4, 2023. https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

Vander, M., & Rotman, D. (2024). SEC cybersecurity disclosure rules: Cracking the code on materiality and reporting, KPMG Media News. February 27, 2024. https://kpmg.com/us/en/media/news/sec-cybersecurity-disclosure-rules-2024.html

Wang, Y., & Fan, W. (2014). R&D reporting methods and firm value: Evidence from China. *Chinese Management Studies, 8*(3), 375-396. https://doi.org/10.1108/CMS-01-2013-0019

Xu, S., Chen, X., Li, A., & Xia, X. (2020). Disclosure for whom? Government involvement, CSR disclosure and firm value. *Emerging Markets Review, 44*. https://doi.org/10.1016/j.ememar.2020.100717

Zukis, B. (2024). Companies are already not complying with the new SEC cybersecurity incident disclosure rules. *Forbes Leadership Strategy*, March 4, 2024. https://www.forbes.com/sites/bobzukis/2024/03/04/companies-are-already-not-complying-with-the-new-sec-cybersecurity-incident-disclosure-rules/?sh=258c7d8b5273