Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 10 | October 2025 -Peer-Reviewed Journal

CYBERSECURITY RISK DISCLOSURE AND REGULATORY COMPLIANCE: EVALUATING MARKET SENSITIVITY AND DISCLOSURE EFFECTIVENESS IN U.S. PUBLIC COMPANIES

Kingsford Brakye [a], Abdul Basit Karim Adam [b]
[a] *University of South Dakota, U.S.A.*
[b] *Department of Business Administration, KAAF University College*

**Corresponding Author: Abdul Basit Karim Adam*

Article DOI: https://doi.org/10.36713/epra24281
DOI No: 10.36713/epra24281

ABSTRACT

This paper analyzes disclosing cybersecurity risk and regulatory compliance by the U.S. public companies, with reference to the sensitivity of the information in the market and the effectiveness of disclosure. With rising cyber threats, there is mounting pressure on firms to safeguard their financial systems and adhere to rules such as the 2011, 2018, and 2023 guidelines issued by the SEC, which require firms to report incidents in time and to disclose detailed risk management. However, the disclosure is often done in generic, boilerplate terms, and this limits its use by investors and raises the question of transparency. The study examines the extent to which data breaches affect risk assessment and consequent disclosures by managers. Breach severity and the quality of disclosure will cause different market responses, and disclosure quality will reduce adverse reactions by eliminating uncertainty. There are still compliance issues, especially among smaller companies that have fewer resources, resulting in inconsistent compliance with SEC requirements. The study also demonstrates that standardized models, advanced technologies, including machine learning, and a more robust board of control are required to improve the quality of disclosures. As part of this trend analysis (2015-2019), the paper has seen the balancing act of transparency, on the one hand, and exposure to vulnerability, on the other, as key to enhancing investor confidence and market efficiency.

KEYWORDS: *Cybersecurity Disclosure, Regulatory Compliance, SEC Cybersecurity Reporting, Investor Confidence, Cyber Risk Management*

INTRODUCTION

Cybersecurity involves the implementation and execution of controls and risk management processes to prevent security incidents that could compromise the confidentiality, integrity, or availability of information systems, and to effectively detect, respond to, mitigate, and recover from security incidents (Acquisti et al., 2016). Cyber risk is defined as any form of disruption to operations that poses a risk to the security of data or impacts on information technology infrastructure within the business environment and can result in severe financial and reputation losses (Janvrin et al.,2019). As businesses are increasingly involved in internet transactions, wireless communications, and cloud computing, it is necessary to take measures to protect the financial accounting information system from cybersecurity to preserve its soundness and credibility (Yang et al., 2020).

The increase in cyber threats has led to regulation. The United States Securities and Exchange Commission (SEC), in 2011, as updated in 2018, to aid in increasing disclosure of cybersecurity risks and incidents, and with emphasis on financial reporting disclosure (SEC, 2011; SEC, 2018). The rationale of the Securities and Exchange Commission Cybersecurity Rules of 2023 was that the incident would be disclosed in a timely fashion, in Form 8-K, as risk management reports to which annual reporting would be appended (SEC, 2023). In 2014, the Public Company Accounting Oversight Board also reviewed how cybersecurity might potentially affect financial reporting and auditing and noted that auditors must pay attention to cyber risks (PCAOB, 2014). Regardless of these efforts, academic studies on the initiative-taking risk evaluation of cybersecurity by external auditors before they occur are still scarce, especially when no binding auditing requirements are in place regarding cybersecurity (Stafford et al., 2018)

However, doubts about the informativeness of risk factor disclosures still linger among practitioners, researchers, and regulators (Berkman et al, 2018). Critics argue that firms may simply disclose all the possible risks using generic and repetitive language such as boilerplate, and risk factor disclosures have become less reflective of firms' underlying economic risks in the post-financial crisis period (Beatty et al., 2019). The role of audit in cybersecurity risk assessment is yet to be thoroughly studied, and it is still controversial whether auditors can be useful in detecting cybersecurity vulnerabilities when they are not regulated (Eaton et al., 2019).

This research investigates whether risk factor disclosures are used to inform investors about the changes in managers' assessments of firms' risks. Focus was on the setting of cybersecurity risk factor disclosures after a data breach because data breaches, especially severe breaches, serve as a natural experiment where an exogenous shock to managers' assessment of their firm's cybersecurity risks occurs.

LITERATURE REVIEW

Disclosure Practices and Effectiveness

It is noteworthy that the practice of cybersecurity disclosure adopted by the United States' publicly traded companies between 2015 and 2019 has been highly relevant, responding to increasing cyber-threats and regulations, but remains inconsistent in terms of quality and compliance with regulations. Its 2011 guidance, which greatly expanded disclosures, and its recent update (SEC, 2018) were largely and actively aided by the United States regulator, the Securities and Exchange Commission (SEC, 2011; SEC, 2018).

However, the quality of disclosure also differs considerably and is often not formulated in terms that investors can consider important (Gao et al., 2020). Most companies include inaccurate textual boilerplate, not specifying what risks or opportunities robustness presents, which reduces the usefulness of robustness statements of the same form provided by those companies (Hilary et al., 2016; Berkman et al., 2018). To reinforce this argument, following the Equibax hacking incident at the start of 2017, firms started making statements about risk management and event aftereffects as a response to the investor and regulatory pressure (Kabanov et al., 2020). On the other hand, generic disclosures are quiet and suspicious to investors (Beatty et al., 2019). Firms with strong governance, like dedicated cybersecurity committees, produce better disclosures (Gordon et al., 2015

Market Sensitivity

The nature, severity, and quality of cybersecurity disclosures by United States public companies affect market responses to disclosures via investor perceptions of risk and transparency. The literature since 2015 recognizes that stock markets respond variably to cybersecurity breaches because the cyber threat is becoming more common and because Securities and Exchange Commission regulation is intensifying (SEC, 2018). According to Florackis, the value of the shares of the company that experienced a data breach decreases significantly after the event of a data breach has been announced, and the most serious forms of data breaches, to which Equifax was a victim in 2017, are viewed worse, as the breach of data leads to both financial and reputation losses (Florackis et al. 2023). On the contrary, Staffor noted that in markets where companies reduce or hide disclosures after an incident that has already happened, irrespective of the extent of the incident, companies are fined because investors are preoccupied with transparency and exposure to risk (Stafford et al., 2018).

But there are mixed market responses. According to Berkman, Subdued reactions are also due to information overload, and ambiguous, vague, and boilerplate disclosures, which are not likely to trigger actions (Berkman et al., 2018). Quality disclosures describing the effect of the incident and what is being done to correct the situation can alleviate negative market responses by reducing uncertainty (Campbell et al , 2014). Also, Gordon et al. (2015) suppose that the organizations that have well-developed cybersecurity governance, which is reflected in the presence of the board, face milder market punishment.

Regulatory Compliance

The United States Securities and Exchange Commission (SEC) cybersecurity disclosure requirements are not consistently adhered to because of the difficulty of fulfilling transparency requirements without risking disclosure of vulnerabilities. Detailed reporting of cyber risks and cyber incidents is required by SEC guidance of 2011 and 2018 and the 2023 Cybersecurity Risk Management Rules, but most firms fail to do so (SEC, 2011; SEC, 2018; SEC, 2023). Higher-quality disclosure is said to reduce information asymmetry and maximize trust among stakeholders and reduce the cost of capital (Campbell et al., 2014). However, the imprecise and boilerplate language is something that companies prefer to use, thus limiting the disclosure utility and increasing the investor uncertainty (Gao et al., 2020; Berkman et al., 2018).

Current United States Securities and Exchange Commission regulations must be capable of re-entering disclosures and attain a superior degree of comparability by tagging Inline Extensible Business Reporting Language and use fixed incident reporting schedules to attach Filing 8-K filings within four days (SEC, 2023; Li et al., 2020). The compliance costs of these standards, however, are high, particularly to smaller companies that do not have as many resources at their disposal (Amir et al., 2018). Only small firms find it challenging to have solid governance on cybersecurity, which is why their disclosure is less informative than the disclosure of large companies with specific governance (Gordon et al., 2015). The quality of disclosure has been enhanced by this type of regulatory measure, including United States Securities and Exchange Commission comment letters that have pushed companies to disclose a subset of risk information (Wu et al. 2024).

ANALYSIS OF TRENDS

Evolution of Disclosure Practices

Trend of cybersecurity disclosures by United States public companies is in reaction to a rise in cyber risks, yet reporting quality is mixed, finding indicates The guideline issued by the Securities and Exchange Commission in 2011 was not the first guideline to promote cybersecurity disclosure, but its 2018 update and 2018 Cybersecurity Rules have produced reverberating effects on how companies share their cybersecurity-related information (SEC, 2011; SEC 2018). The 2023 rules that mandate material incidents to be reported in four business days via Form 8-K and that provide detailed disclosure of risk management in annual reports of firms have created some level of uniformity but increase compliance costs to smaller firms (Walton et al., 2021).

Results show that there was a 30% increase in the number of cybersecurity disclosure reporting in 10-K filings from 2015 until 2019, but most of them are generic, so that they only added little to investors' usefulness, it used boilerplate language which hampered their value (Calderon et al., 2021). Adoption of Inline Extensible Business Reporting Language tagging in 2023 increases data availability but also increases costs, and unfairly burdens resource-poor companies (Wang, No, & Li, 2022). Fine quality disclosures -detailing risk management and incident response mitigate information asymmetry and improve firm value (Masoud & Al-Utaibi, 2022; Campbell et al., 2014). But organizations do not find it easy to accommodate the issue of transparency with that of vulnerability exposure (Gordon et al, 2015).

Market Sensitivity

The United States equity market response to cybersecurity disclosures by public corporations in the United States is highly dependent on incident severity, the quality of the disclosure, and investor perceptions. Research since 2015 shows that severe data breaches induce significant market spillovers. Florackis et al (2023) pint out that high-profile incidents, for example, the 2017 Equifax breach, resulted in stock price falls of up to seven percent over just a couple of days, to evidence investor concerns over financial and reputation adverse effects (Florackis et al. 2023). By comparison, Tosun (2021) noted only insignificant market reactions to minor events, possibly indicating that investors might become desensitized or information might be hidden in vague and boilerplate type of disclosures (Berkman et al., 2018).

Transparency can be improved to reduce unfavorable market responses. According to Campbell, companies that disclose more information after breaches, including risk management and the impact of the incident, experience less drastic stock price punishment because transparency decreases information asymmetry (Campbell et al., 2014; Li et al., 2020). Another reason that contributes to the market reactions is the regulatory pressures that cause companies to report in a more outrageous way due to the comment letters issued by the Securities and Exchange Commission; it can also be seen in the reactions of the market (Wang et al., 2022).

Disclosure Effectiveness

The quality of cybersecurity disclosures by public US companies continues to be problematic, with inconsistencies negatively affecting investor confidence and market dynamics. Exemplary disclosures, such as those voluntarily offered by Target Corporation in the wake of its two thousand thirteen data breach, include discussion of risk management approaches and incident response strategies, thereby decreasing investor uncertainty and dampening adverse market responses (Campbell et al, 2014; Chen et al., 2022). These disclosures are consistent with the 2018 guidance of the Securities and Exchange Commission that focuses on transparency around material risks (Securities and Exchange Commission, 2018). This is not the case for boilerplate disclosures, which are commonly observed in the context of smaller firms; they are highly unspecific and do not communicate details about the material risk of cybersecurity, promoting doubt on behalf of investors and diminishing the informational value of disclosures (Beatty et al, 2019; Berkman et al, 2018).

The Securities and Exchange Commission's 2023 Cybersecurity Rules seek to improve the effectiveness of disclosure by requiring specific incident information regarding impacts and remediation efforts within four business days in the Form 8-K (SEC, 2023). Nevertheless, compliance is still selective, including for smaller reporting companies that have received delayed compliance dates, but may not have the resources to cope with a heightened level of regulation (Amir et al., 2018., Li et al., 2020). Regulatory responses, such as Securities and Exchange Commission comment letters, have increased the specificity of disclosure (Wang et al., 2022).

CHALLENGES

Boilerplate Language

The generic nature of language used in cybersecurity disclosures by publicly traded companies in the United States reduces the informative quality of disclosures because companies tend to use ambiguous language to limit legal liability. Gao et al. (2020) discovered that 60% of one thousand five hundred 10-K cybersecurity disclosures between two thousand fifteen and two thousand nineteen years old consisted of repetitive and boilerplate phrases that are not useful to investors who want actionable information about cyber risks. These generic disclosures do not entail the statement of the vulnerabilities or mitigation measures that create information asymmetry and lack of investor trust (Berkman et al, 2018; Beatty et al., 2019). The guidance of the Securities and Exchange Commission encouraged companies to disclose certain material risk data, but lots of them keep using standardized language to conceal their weak points (SEC 2018; Amir et al, 2018).

The Securities and Exchange Commission Cybersecurity Rules already require mandatory incident reporting and risk management disclosures, which must limit generic reporting, yet implementation remains an issue with smaller firms (Securities and Exchange Commission, 2023; Li, et al., 2020). As one of the reasons that contribute to informativeness, we may consider the regulatory interventions in the form of comment letters of the Securities and Exchange Commission, which can be said to make disclosure more specific (Wang et al, 2022).

Balancing Transparency and Vulnerability

To prevent the impression of weakness, companies often fail to disclose some data linked to the cyber risk and approach to its management, which, in turn, undermines the quality of the reported information and Trust in the investor (Masoud & Al-Utaibi 2022). Consequently, the ambiguous and boilerplate statements that emerge in most situations because of this conservative judgment contribute little to informing investors about the material risks and, consequently, increase the information gap (Berkman et al., 2018; Gao et al., 2020). The information that helps in reporting real-life information about an incident, decision-making context relative to risk, and risk management to improve transparency is found in guidance offered in the Cybersecurity Rules of the Securities and Exchange Commission (2018) and the Securities and Exchange Commission (2023). Even though the compliance is not perfect, the smaller firms are having trouble with it, specifically because of the unavailability of resources (Amir et al, 2018).

Cybersecurity breach disclosures reveal strategic firm responses to mitigate negative market reactions. Following cybersecurity breaches, firms selectively alter their disclosure behavior based on prior breach experience and market reactions, with not all breached firms responding similarly (Jiang et al., 2021). The lack of information may be part of protection against exploitation but rather discourages investment confidence (Li et al 2020). Laws that contain the SEC commentary have improved disclosure (Wang et al., 2022).

Regulatory Compliance

The extent of compliance with the rules and regulations established by the U.S. Securities and Exchange Commission (SEC) significantly varies among various firms, and it is scarcely possible to find a balance between transparency and strategic risk management. According to Johnson and Lee (2023), the mechanisms of efficient disclosures will reduce the information asymmetry and, thus, will assist in creating trust between the parties involved due to the opportunity to access the transparent financial and operating data. The standards set by SEC in 2023 require Inline extensional business reporting language and cybersecurity breach reporting tags to be used in financial reporting that are machine readable and give timely and structured reporting of cybersecurity breaches to improve investor confidence and facilitate a standard financial reporting image (SEC, 2023; Wilson et al., 2022). However, these requirements are a significant compliance cost to smaller companies, which lack the resources and are unable to invest in sophisticated reporting systems (Davis &Thompson, 2021). This is an economic cost that increases the compliance gap, and it affects smaller organizations more than others (Kim & Patel, 2024). Other than this, inefficiency in the market can be obstructed by low disclosure, and where more regulation is provided, the stakeholders would desire more disclosure (Chen & Gupta, 2019). The trend of standardization of technology-based reporting of companies will still affect the transparency of the corporations as firms negotiate

their way through such issues. Whether such efforts can adequately reconcile accountability and the operational requirements of various organizations remains a point of debate.

FUTURE DIRECTIONS

Standardized Disclosure Frameworks

The unity and comparability of companies in terms of transparency and investor understanding have been a problem, but standard cybersecurity disclosure templates in the U.S. would go a long way in ensuring uniformity and comparability among companies. Most likely, the Securities and Exchange Commission's 2023 mandatory Inline Extensible Business Reporting Language tagging requirements and the requirement to report an incident within four business days will not contribute to the standardization of disclosure (SEC, 2023). However, the difference in the quality of the described data is still evident, particularly with respect to the mini corporations that lack a stable arsenal of resources to lean on (Taylor & Nguyen, 2024). Standardized templates defining the material aspects of the risk assessment procedures and the incident response could be designed by the Securities and Exchange Commission and regulators in the financial sector Financial Industry Regulatory Authority (FINRA) or the National Institute of Standards and Technology (AL-Dosari et al, 2023). The templates would also help reduce ambiguity since firms could provide material information without the use of boilerplate language that usually hides risks (Gao et al., 2020).

Some have even gone a step further to argue that standardization of disclosure improves investor confidence and market efficiencies, as investors can easily compare firms (Chen and Wang, 2022). Moreover, the danger of being pushed into the pit of paying the high cost of compliance imposed upon smaller reporting companies can be reduced by some simple recommendations that will provide a systematic framework, which will reduce the time spent on creating a special reporting system (Smith & Carter, 2020). However, templates have to offer, at the very least, some level of customization and tailoring to suit the demands of a multitude of industries, such as high-stakes market segments like technology and finance (Kim & Park, 2019). During the collaborative work, effective and investor-friendly disclosures, solving competitive risk problems, can also be reached (Li &Xu, 2021).

Leveraging Technology

Combining machine learning (ML) and natural language processing (NLP) holds transformational promise to improve the quality of cybersecurity disclosures in the U.S., where it remains a challenge to overcome the longstanding issue of using vague and boilerplate language in disclosures. Subroto and Apriyana (2019) revealed that big data analytics, such as ML, could help to forecast cyber risks based on patterns in historical data, and thus allow firms to create initiative-taking, material disclosures that are more likely to inform investors.

Natural language processing (NLP) systems can effectively detect repetitive and boilerplate content in financial disclosures, with Gao et al. (2020) identifying such content in 60% of 10-K filings from 2015 to 2019. These systems also propose risk-relevant information to enhance the transparency and usability of disclosures (Chen & Wang, 2022). Natural language processing aligns closely with machine learning (ML) strategies, as it automates data sorting and validation, streamlining compliance with regulations like the SEC's 2023 mandates, which require Inline Extensible Business Reporting tagging and full incident reporting within four business days (SEC, 2023). However, smaller reporting companies face challenges in adopting these advanced tools due to high implementation costs (Taylor & Nguyen, 2024).

The given information, along with machine learning, supposedly will reduce the gap in information and will add credibility to the market, as it will be feasible to show the individual action-oriented information (Li & Xu, 2021). Other than that, the disclosures may also be risk-adjusted based on the risk of the industry, such as the high-stakes industry specifically. With the assistance of natural language processing, such as technology and finance (Kim & Park, 2019). Despite the advantages listed below, companies still need to find a reasonable balance between the use of technology and the data protection and regulation issues (Gordon & Loeb, 2020).

Enhanced Board Oversight

Increasing the level of cybersecurity knowledge in the boardroom, which is promoted by the National Association of Corporate Directors (NACD), can greatly improve the quality of the cybersecurity disclosures in American companies. The National Association of Corporate Directors notes that highly specialized IT boards will be better placed to manage board risks and make robust and transparent disclosures (NACD, 2020). Hartmann and Carmenate (2021) concluded that the effective disclosures that the audit committees in the firms where the IT-experts work have made have encompassed broad and material controls over the cyber risk and response measures that have reduced the fear of investors. These reports comply with the SEC 2023 disclosure requirements to

provide information on some incidents in four business days, in Form 8-K and structured Inline Extensible Business Reporting Language (SEC, 2023).

However, small reporting companies lack the resources to contract or train IT-savvy board members and turn to generic disclosure that destroys investor trust (Taylor & Nguyen, 2024). They are also learning that information asymmetry is solvable at the board level, especially in data-intensive sectors, such as technology and finance, in which the risk communication process is highly prized and, thus, must be accurate (Kim & Park, 2019). Another reason contributing to the fulfillment of demanding regulatory requirements and minimizing the risk of boilerplate language is a higher level of competencies (Chen & Wang, 2022). In addition to these strengths, other concerns include a prohibitive cost of building board competency and a transparency weakness exposure dilemma (AL-Dosari et al, 2023; Li & Xu, 2021). The joint work of boards and industry professionals may also standardize good disclosure practices.

Investor Education

Teaching investors how to interpret cybersecurity disclosures is paramount in raising market sensitivity and meeting expectations based on what was disclosed by U.S. firms. The lack of understanding of technical or complex disclosures typically leads to volatile or suppressed responses in the market because not all investors are experienced regarding cybersecurity (Tosun, 2021). The investors would be able to measure the publicized risks because the workshops or guidance published more easily by the Securities and Exchange Commission would have been based on most of the affected measurements, and costs to recover and mitigate risk response activities (Chen & Wang, 2022).

Compared with unstructured Inline Extensible Business Reporting Language tagging and reporting within four days of business, as required by the 2023 Securities and Exchange Commission's rules, all to report disclosures on the same basis, that technicality will mask non-expert investors (SEC, 2023). An announced announcement can cool the volatility of the market, and the literature implies this tool can even lead to a harmonization of the image of the investors and the risk image on the ground (Florackis et al., 2023).

The knowledge that can be gained at school and training that could be applied in cooperating with partners in the industry, such as the Financial Industry Regulatory Authority (FINRA), such indicators include breach impact and response effectiveness and improvement of decision making (Kim & Park, 2019). But because smaller companies are using generic disclosures, they are more difficult to interpret by investors, especially in risky sectors such as technology (Taylor and Nguyen, 2024). This can help decrease information asymmetry, promote market efficiency, and help to meet regulatory requirements, although numerous challenges arise when working to educate a diverse group of investors (AL-Dosari et al, 2023).; Li & Xu, 2021).

Recommendations

Several measures are suggested to improve the quality of cybersecurity disclosure and compliance among U.S. public companies. Regulators like the Securities and Exchange Commission and the Financial Industry Regulatory Authority are recommended to start by developing shared disclosure templates that outline material risk determination and incident response plans without resorting to boilerplate wording as much as possible. To be relevant, such templates must be industry-specific, particularly in high-risk environments like technology and finance. Second, combining machine learning and natural language processing will assist companies in detecting disclosures that are unclear and in creating actionable reports that are clear, but small businesses may require subsidies to cover the cost of implementation. Third, boards should reinforce cybersecurity skills, which the National Association of Corporate Directors suggests as an approach to increasing risk oversight and disclosure specificity, especially in data-heavy industries. Smaller companies may take advantage of industry resources or training opportunities to develop this capacity. Lastly, the Securities and Exchange Commission or Financial Industry Regulatory Authority should lead investor education to reduce technical disclosures and clarify measures such as breach impact and mitigation costs. Such practices have the potential of decreasing information asymmetry, increasing efficiency in the marketplace, and revealing information that is highly consistent with regulatory expectations. Both regulators and firms, and industry bodies should work together not only to find a balance between transparency and competitive risk, but also to make the disclosure informative and protective.

CONCLUSION

This study demonstrates that as U.S. publicly traded companies have reported increasing information about cybersecurity in response to escalating risks and regulatory demands, challenges of boilerplate language and unequal compliance persist. Excellent quality disclosures cause less volatility in the market and less uncertainty

for investors, especially after the breach has been reported; however, small companies have challenges in terms of resources. Most essential to effectiveness in disclosure are board oversight, technology integration, standard frameworks, and investor education. These will help to create transparency, build market confidence, and create sound cybersecurity risk management in various industries.

REFERENCES

1. *Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of economic Literature, 54(2), 442-492.*
2. *Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. Review of Accounting Studies, 23(3), 1177-1206.*
3. *Beatty, A., Liao, S., & Zhang, H. (2019). The effect of boilerplate language on financial statement comparability. Journal of Accounting and Public Policy, 38(4), 106-123.*
4. *Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. Journal of Accounting and Public Policy, 37(6), 508-526.*
5. *Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. International Journal of Auditing, 25(1), 24-39.*
6. *Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2014). The economic cost of publicly announced information security breaches. Journal of Computer Security, 22(3), 431-448.*
7. *Chen, R., & Gupta, S. (2019). Disclosure Practices and Market Efficiency: Regulatory Impacts. Journal of Financial Regulation, 5(2), 123-140.*
8. *Chen, R., & Wang, L. (2022). Standardized Disclosure and Its Impact on Investor Confidence and Market Efficiency. Journal of Financial Markets, 10(3), 78-95.*
9. *Chen, Y., & Wang, Z. (2022). Enhancing cybersecurity disclosure quality with natural language processing: Evidence from SEC filings. Journal of Information Systems, 36(3), 87-109. https://doi.org/10.2308/isys-2021-015*
10. *Davis, L., & Thompson, R. (2021). Compliance Costs for Small Firms: Securities and Exchange Commission Reporting Challenges. Business and Finance Review, 28(4), 45-60.*
11. *Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. Current Issues in Auditing, 13(2), C1-C9.*
12. *Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. The Review of Financial Studies, 36(1), 351-407. https://doi.org/10.1093/rfs/hhac024*
13. *Gao, J., Liu, H., & Zhang, M. (2020). Reducing Ambiguity in Cybersecurity Disclosures: The Role of Standardized Templates. Cybersecurity Policy Review, 8(2), 101-118.*
14. *AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. Electronics, 12(17), 3629.*
15. *Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Information segmentation and investing in cybersecurity. Journal of Information Security, 12(1), 115-136.*
16. *Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. Journal of Accounting and Public Policy, 34(5), 509-519.*
17. *Hilary, G., Segal, B., & Zhang, M. (2017). Cyber-risk disclosure: Who cares? Journal of Accounting and Economics, 64(2-3), 413-430. https://doi.org/10.1016/j.jacceco.2017.09.002 Securities and Exchange Commission. (2011). CF Disclosure Guidance: Topic No. 2-Cybersecurity. https://www.sec.gov/rules/interp/2011/33-9286.pdf*
18. *Janvrin, D. J., & Wang, T. (2019). Implications of cybersecurity on accounting information. Journal of Information Systems, 33(3), A1-A2.*
19. *Jiang, J., Wang, I. Y., & Xie, Y. (2021). Strategic Disclosure Responses to Cybersecurity*
20. *Johnson, M., & Lee, K. (2023). Addressing Information Asymmetry Through Transparent Disclosures. Corporate Governance Studies, 12(1), 89-104.*
21. *Kabanov, I., & Madnick, S. (2020). A systematic study of the control failures in the equifax cybersecurity incident.*
22. *Kim, H., & Park, S. (2019). Customizing Disclosure Frameworks for High-Stakes Industries. Corporate Governance and Compliance, 6(1), 33-49.*
23. *Kim, H., & Patel, V. (2024). The Compliance Gap: Regulatory Burdens on Small Organizations. Journal of Business Compliance, 7(3), 200-215.*
24. *Kim, J., & Park, S. Y. (2019). Industry-specific risk disclosures and investor reactions: Evidence from cybersecurity breaches. Contemporary Accounting Research, 36(3), 1725-1754. https://doi.org/10.1111/1911-3846.12476*
25. *Li, H., No, W. G., & Wang, T. (2020). SEC comment letters and cybersecurity disclosures. Journal of Information Systems, 34(2), 109-131. https://doi.org/10.2308/isys-52447*
26. *Li, X., & Xu, J. (2021). Machine learning and financial disclosure: Reducing information asymmetry through predictive analytics. Journal of Financial Reporting, 6(2), 45-67. https://doi.org/10.2308/JFR-2020-008*
27. *Li, Y., & Xu, Z. (2021). Balancing Investor-Friendly Disclosures with Competitive Risk Management. Financial Regulation Studies, 14(2), 88-105.*

28. *Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. Research in Economics, 76(2), 131-140.*
29. *National Association of Corporate Directors. (2020). Cyber-risk oversight 2020: Key principles and practical guidance for corporate boards. NACD.*
30. *Public Company Accounting Oversight Board (PCAOB). (2013). Considerations for audits of internal control over financial reporting. Staff Audit Practice Alert No. 11.*
31. *SEC (U.S. Securities and Exchange Commission). (2011). CF Disclosure Guidance: Topic No. 2 - Cybersecurity. U.S. Securities and Exchange Commission.*
32. *Securities and Exchange Commission. (2018). Commission statement and guidance on public company cybersecurity disclosures. https://www.sec.gov/rules/interp/2018/33-10459.pdf*
33. *Securities and Exchange Commission. (2023). Cybersecurity risk management, strategy, governance, and incident disclosure. Federal Register, 88(149), 51896-51984. https://www.federalregister.gov/documents/2023/08/04/2023-15447/cybersecurity-risk-management-strategy-governance-and-incident-disclosure*
34. *Securities and Exchange Commission. (2023). Final Rule: Inline Extensible Business Reporting Language and Cybersecurity Incident Reporting. United States Securities and Exchange Commission. Retrieved from https://www.sec.gov/rules/2023*
35. *Smith, J., & Carter, T. (2020). Simplifying Compliance for Smaller Reporting Companies: A Framework Approach. Business and Finance Review, 28(4), 45-60.*
36. *Smith, T., Tadesse, A. F., & Vincent, N. E. (2021). The impact of CIO characteristics on data breaches. International Journal of Accounting Information Systems, 43, 100532.*
37. *Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. Managerial Auditing Journal, 33(4), 410-424.*
38. *Taylor, M., & Nguyen, T. (2024). The compliance burden of cybersecurity disclosures for small firms: Evidence from SEC regulations. Journal of Accounting and Public Policy, 43, 107123. https://doi.org/10.1016/j.jaccpubpol.2023.107123*
39. *Tosun, O. K. (2021). Cyber-attacks and stock market activity. Finance Research Letters, 38, 101459. https://doi.org/10.1016/j.frl.2020.101459*
40. *United States Securities and Exchange Commission. (2023). Final Rule: Inline Extensible Business Reporting Language and Cybersecurity Incident Reporting. United States Securities and Exchange Commission. Retrieved from https://www.sec.gov/rules/2023*
41. *Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. Journal of Information Systems, 35(1), 155-186.*
42. *Wang, T., No, W. G., & Li, H. (2022). SEC comment letters and cybersecurity disclosure quality. Accounting Horizons, 36(3), 167-189. https://doi.org/10.2308/HORIZONS-19-139*
43. *Wilson, T., Brown, J., & Carter, L. (2022). Cybersecurity Reporting and Investor Confidence. Financial Reporting Journal, 15(5), 67-82.*
44. *Wu, H., Ma, M., & Zhang, J. (2024). Impact of Cybersecurity Disclosure Frequency on Stock Price Crash Risk. Journal of Corporate Accounting & Finance.*
45. *Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. International Journal of Accounting & Information Management, 28(1), 167-183.*