Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 374-384

ADVANCED INTERNATIONAL JOURNAL OF BUSINESS, ENTREPRENEURSHIP AND SMES (AIJBES)
www.gaexcellence.com/aijbes

CYBERSECURITY RISK DISCLOSURE IN ANNUAL REPORTS: A CONCEPTUAL FRAMEWORK WITH INSIGHTS FROM MALAYSIA

Ros Amalina Zakaria[1]*, Azilawati Abdullah @ Ab Aziz[2], Nor Asmawani Che Hassan[3]

[1]Faculty of Accountancy, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Malaysia
amalina86@uitm.edu.my https://orcid.org/0009-0007-5323-1231
[2]Faculty of Accountancy, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Malaysia
azila430@uitm.edu.my https://orcid.org/0009-0003-9222-5070
[3]Faculty of Accountancy, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Malaysia
asmawani@uitm.edu.my https://orcid.org/0009-0007-6945-3779
*Corresponding Author

Article Info:

Article history:
Received date: 21.06.2026
Revised date: 14.07.2027
Accepted date: 28.07.2026
Published date: 10.09.2026

To cite this document:

Zakaria, R. A., Aziz, A. A. A., & Hassan, N. A. C. (2026). Cybersecurity Risk Disclosure in Annual Reports: A Conceptual Framework with Insights from Malaysia. *Advanced International Journal of Business Entrepreneurship and SMEs, 8* (29), 374-384.

Abstract:

As firms become increasingly dependent on digital technologies, cybersecurity has emerged as a critical governance and reporting issue. Consequently, stakeholders are demanding more transparent and decision-useful cybersecurity risk disclosure (CRD). Although regulatory expectations for cybersecurity reporting have increased, prior studies indicate that CRD remains largely boilerplate, inconsistent, and insufficient for stakeholder decision-making. Moreover, limited research has developed an integrated theoretical framework explaining the factors that influence the quality of CRD, particularly in emerging markets. This study proposes an integrated conceptual framework that explains how governance mechanism, regulatory pressures, and proprietary cost considerations jointly influence the quality of cybersecurity risk disclosure. Drawing on signalling theory, proprietary cost theory, and corporate governance theory, the proposed framework examines how board cybersecurity expertise, regulatory enforcement, and proprietary cost consideration shape firms' cybersecurity disclosure decisions. The model represents firm's selective disclosure of cybersecurity information, providing testable propositions for future empirical work. Malaysia provides a distinctive research context because of its concentrated ownership structure, varying levels of board cybersecurity expertise, and evolving regulatory expectations under Bursa Malaysia and the Malaysian Code of Conduct Governance (MCCG). The proposed framework extends the accounting and information systems literature by providing a theoretically grounded

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 374-384

basis for examining cybersecurity risk disclosure risk disclosure quality in emerging markets and offers testable propositions for future empirical research.

DOI: 10.35631/AIJBES.829020 **Keyword:**

Annual Reports, Corporate Governance, Cybersecurity Disclosure, Malaysia, Proprietary Cost Theory, Signalling Theory.

Introduction

Corporate organizations are now significantly exposed to risk of cybersecurity as nowadays majority of them are adopting cloud computing, interrelated enterprise system as well as the artificial intelligence (Sun & Chang, 2022; Parra & Rossi, 2023). The risk of cybersecurity or the threat to the cyber currently become indicator that can negatively affect the firm value, the confidence of the investors and its perpetual continuity, whether through financial or operation, or both. There are regulatory efforts in place, however, organization still finding ways on how to effectively convey the cybersecurity risk. For instance, F5, Inc. revealed that a sophisticated nation-state threat actor had long-term unauthorized access to its systems, including its fundamental BIG-IP product development environment, as reported by Hagens Berman in 2025. This revelation sparked investor scrutiny and a precipitous decline in share price. This situation indicates that it is difficult to disclose a timely and informative cybersecurity information even for well-equipped organizations.

Responding to risk, regulatory bodies around the world came out with their own action. As we can see, in U.S, the U.S Securities and Exchange Commission (SEC) in 2023 has mandatorily required the organizations to disclose their cybersecurity information, where the firms need to disclose the governance structure, the process of the risk management as well as significant incidents related to cybersecurity issues (SEC, 2024). Unfortunately, studies reported that the disclosure were not as required, where the firms only disclose boilerplate statement which limit useful information needed to make decision (Gauch et al., 2025; Chen et al., 2023). That kind of disclosure only left the investors and the analyst in difficulty to evaluate the cybersecurity risk management, due to the inadequate depth, specificity and projections.

While in a country like Malaysia, the disclosure quality is affected by the uneven governance maturity, limited cybersecurity expertise and concentrated ownership (Ng & Yap, 2022; Khadim & Kakar, 2025). The risk disclosure is actually been promoted by the Malaysia Code of Corporate Governance (MCCG) and Bursa Malaysia, however the development of the cybersecurity guideline are underdeveloped. Due to that, the disclosure quality among Malaysian firms are vary, which making it hard for the investor to access the risk.

This paper proposed a conceptual framework that explains the factors influencing the quality of cybersecurity risk disclosure in the context of Malaysian as the emerging market. The proposed conceptual framework shows how board cyber expertise, board independence, regulatory enforcement strength, proprietary cost considerations and Malaysian institutional features interact to influence disclosure practices, using a multi-theoretic framework drawing on signalling theory, proprietary cost theory and corporate governance perspective. By doing this, the study offers a methodical theoretical framework for comprehending disclosure quality variability and suggests testable proportions for further investigation.

Literature Review

Cybersecurity Risk Disclosure in Corporate Reporting

With the increasing numbers and seriousness of cyber incidents and the increasing regulatory expectations, CRD (cybersecurity risk disclosure) has become a crucial area of corporate reporting (Moll & Yigitbasioglu, 2025). Nowadays, companies are working in highly digitalised environments where cyber security risks can have a significant impact on financial performance, continuous of operation and confidence of the stakeholders. Therefore, CRD is no longer just a technical but a strategic reporting issue that are closely followed by investors and analysts.

Even though the SEC has come out with the mandatory disclosure requirement, but the cybersecurity disclosure informativeness actually remains limited (Block, 2025; Chen et al., 2023). It is evidence that many firms do not offering details on risk management process, governance structure or actual incidents. They just provide symbolic or general disclosure that define standard IT safeguard only or just repeat boilerplate statements. Resulting from that, the information asymmetry remains large, and investors are less equipped with useful information in making decision.

Research also finds variations across industry and institution. It is hypothesized that firms within a regulated industry (e.g. Finance) will more likely disclose detailed CRD than those who only provide general risk statements. Such quality is also attributed to corporate governance structure, board composition and knowledge, as well as stakeholder pressure. These imply that CRD quality is not only a function of regulatory compliance, but also corporate strategic choices and governance considerations, hence a theoretical framework is needed to explain such inconsistency in disclosure quality.

Determinants of Cybersecurity Disclosure Quality

Corporate governance has long been cited as a key determinant of CRD quality. Board's knowledge in terms of cybersecurity may allow directors to fully understand complex risks, thereby facilitating them to better challenge management assertions (Alodat et al., 2024;

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 374-384

Khadim & Kakar, 2025). Similarly, independent boards and effective audit committee provide enhanced monitoring capabilities that can contribute to substantive, as opposed to token, disclosures (Smaili & Radu, 2023). However, in some firms, governance is largely symbolic, as companies implement governance structure with only ceremonial intent, thereby not truly concerned about transparency (Jameel et al., 2025).

Regulatory enforcement also plays an important role in CRD disclosure quality. Strong enforcement lead to better depth and timeliness of CRD, while weak enforcement usually results in minimal disclosure behaviour (Deloitte, 2025). Besides that, concentrated ownership in emerging market can reduce external monitoring, which become a weakening incentive for high-quality disclosure (Khadim & Kakar, 2025). These findings suggest that both internal governance mechanisms as well as external regulatory pressures mutually shape CRD practices, and this become the rationale for integrating these determinants in a conceptual framework.

Theoretical Foundations

Within the signalling theory, firms are expected to use CRD to signal their capabilities in effective governance and risk management to reduce information asymmetry and improve credibility (Godewatta et al., 2025). Proprietary cost theory suggests that companies may limit disclosure to avoid revealing sensitive cybersecurity practices that could be exploited by competitors or attackers (Vo & Pham, 2025).

The interaction of these theories explains the reason why firms prefer signaling, but not full, disclosure. Good governance mechanism would lead to high quality disclosure, whereas proprietary cost consideration might prevent the information disclosed in a great detail or precise level. Therefore, understanding the conflicts is crucial in explaining the variations in disclosure quality across firms.

Malaysian Institutional Context

As an emerging market, Malaysia offers a unique backdrop for the study of CRD. Concentrated ownership structure and heterogeneous board knowledge levels would imply reduced external and internal monitoring, thereby yielding low CRD quality (Ng & Yap, 2022; Khadim & Kakar, 2025). Similarly, specific guidance for cybersecurity disclosure is not provided even though MCCG mandates for risks reporting. Besides, pressures of digital transformation (e.g. AI adoption and technostress) influence a firm's decision regarding investment on cybersecurity governance and reporting (Parra & Rossi, 2023; Sun & Zhang, 2022). These institutional pressures in the Malaysian context are thus expected to drive significant heterogeneity in disclosure quality.

Research Methodology

The purpose of this conceptual research is to develop a theoretical framework that shows the factors determining the quality of cybersecurity risk disclosure (CRD) in the annual reports of companies within Malaysian emerging market setting. In this study, a literature review was conducted to draw upon a range of studies on corporate governance, regulatory enforcement, proprietary cost factors and institutional settings. Specifically, it combines signals theory and proprietary cost theory with relevant corporate governance and regulatory concepts to construct

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 374-384

the conceptual model. The paper presents and elaborates on arguments about how board cybersecurity knowledge, board independence, regulatory enforcement quality, proprietary cost concern and Malaysian institutional environment influence CRD quality. The methodology highlights synthesis and integration of previous findings to develop the framework.

Research Gap

There exists a significant gap in the literature regarding CRD although the interest has increased among researchers and practitioners. Firstly, the need for a holistic framework that integrates governance, regulatory and proprietary cost factors have yet to be filled. Secondly, previous research has typically measured CRD quality in terms of its quantity, as firms tend to demonstrate compliance rather than informative disclosures. Thirdly, lack of empirical evidence on emerging markets is apparent, and for Malaysia, its peculiar institutional environment may strengthen or weaken firms' disclosure choices.

Proposed Conceptual Framework

In order to breakdown the variables that influence the quality of cybersecurity risk disclosure (CRD) in annual report, this paper proposed a conceptual framework as can be seen in the Figure 1 below. The framework incorporates signalling theory, proprietary cost theory, and corporate governance perspectives, showing thar cybersecurity disclosure is not merely a technical issue in reporting but it is a crucial or tactical governance decision. Organization may choose to show report that illustrate strong risk management system as well as governance, but when the information is sensitive or can lead to strategic risk, the may also curtail the disclosure.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 374-384

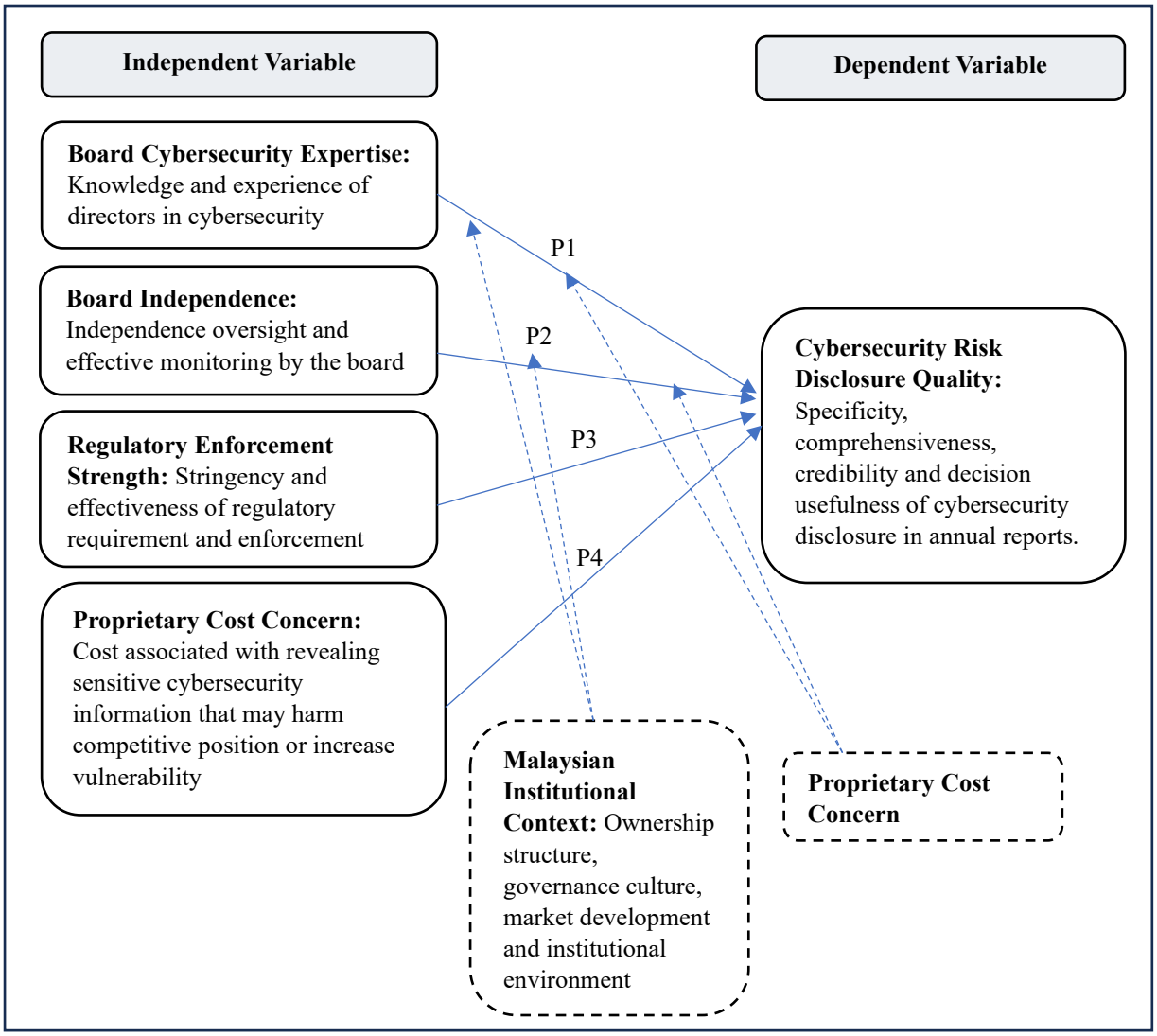

Figure 1: Conceptual Framework of the Factors Influencing Auditor Independence

The framework suggests four main variable that can affect the CRD quality which are board cybersecurity expertise, board independence, regulatory enforcement strength, and proprietary cost concerns. Board expertise and independence represent the internal governance, while external institutional pressure is indicated by regulatory enforcement. Firms with strong governance can still limit their disclosure when it is constrained by the propriety cost concern. In addition to that, there are moderating effect that were included in the framework to see how the Malaysian institutional context influences the disclosure in term of governance, and how proprietary cost concerns effect the positive relationship of the governance on the CRD quality.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 374-384

Key Constructs in the Framework

Table 1: Definitions of Key Constructs in the Conceptual Framework

Construct	Definition	Theoretical Role
Cybersecurity Risk Disclosure Quality (CRD Quality)	Refers to the extent to which annual report disclosures provide specific, relevant, transparent, and decision-useful information regarding cybersecurity risks, governance structures, incident response, cybersecurity policies, and future risk preparedness. In this paper, disclosure quality is evaluated based on the informativeness and specificity of disclosure rather than disclosure quantity alone.	**Dependent Variable**
Board Cybersecurity Expertise	Refers to the presence of directors with professional knowledge, qualifications, or experience in cybersecurity, information technology, digital governance, or information systems. Directors with cybersecurity expertise are expected to improve board oversight and strengthen the quality of cybersecurity reporting.	**Independent Variable**
Board Independence	Refers to the independence and lack of conflicts of interest among board members relative to executive management. Independent directors are perceived to improve monitoring and enhance the substance and transparency of cyber risk disclosures.	**Independent Variable**
Regulatory Enforcement Strength	Refers to the intensity with which the regulator establishes disclosure requirements, enforces compliance with disclosure regulations, and penalizes for non-compliance. Strong regulatory enforcement mechanisms will likely enhance quality of disclosures by signaling to firms that non-compliance will be punished.	**Independent Variable**
Proprietary Cost Concerns	Refers to the perceived danger that disclosing sensitive details about cybersecurity exposures might signal vulnerabilities to cyber-attackers or competitors and may reveal defense mechanisms and strategies used by the firm. These concerns might deter the disclosure of cybersecurity risks.	**Independent Variable / Moderating Variable**
Malaysian Institutional Context	Refers to contextual institutional characteristics, including concentrated ownership structures, varying governance maturity, evolving cybersecurity reporting norms, and regulatory	**Moderating Variable**

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 374-384

	expectations within Malaysia. These institutional factors may influence the effectiveness of governance mechanisms in improving disclosure quality.	

Table 1 shows that CRD quality is influenced by internal governance mechanisms and external institutional factors. Board's cybersecurity knowledge, board's independence and regulatory enforcement will positively impact on disclosure quality whereas the disclosure practice will likely be negatively affected by proprietary cost concerns. There will be a moderating effect on these factors by unique institutional traits of the Malaysian emerging market.

Propositions Development

Six propositions that can explain the quality of CRD were developed using the signaling theory, proprietary cost theory, and the literature of corporate governance. These propositions along with hypotheses and empirical supports are presented below.

Table 2: Research Propositions and Supporting Literature

Proposition	Statement	Justification	Previous Studies
P1	Board cybersecurity expertise positively influences cybersecurity risk disclosure (CRD) quality.	Directors with information system or cybersecurity or expertise are better equipped to understand cyber risks, evaluate cybersecurity governance, and challenge management regarding disclosure adequacy. Such expertise improves board oversight and promotes more specific and decision-useful reporting.	Alodat et al. (2024); Khadim and Kakar (2025); Smaili and Radu (2023)
P2	Board independence positively influences cybersecurity risk disclosure (CRD) quality.	Independent directors strengthen accountability and monitoring mechanisms by encouraging greater transparency and reducing managerial opportunism. Independent oversight may discourage symbolic disclosure and improve substantive cybersecurity reporting.	Smaili and Radu (2023); Jameel et al. (2025); Chen et al. (2023)
P3	Regulatory enforcement strength positively influences cybersecurity risk	Stronger regulatory monitoring and clearer disclosure expectations encourage firms to provide more detailed and structured	Deloitte (2025); Gauch et al. (2025); Chen et al. (2023)

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 374-384

	disclosure (CRD) quality.	cybersecurity reporting to avoid compliance and reputational risks.	
P4	Proprietary cost concerns negatively influence cybersecurity risk disclosure (CRD) quality.	Firms may limit disclosure if they believe cybersecurity information could reveal vulnerabilities, expose strategic systems, or increase risks of cyberattacks. This creates a trade-off between transparency and security.	Vo and Pham (2025); Godewatta et al. (2025); Chen et al. (2023)
P5	Malaysian institutional context moderates the relationship between governance factors and cybersecurity risk disclosure (CRD) quality.	Institutional factors such as concentrated ownership, governance maturity, and evolving disclosure norms may strengthen or weaken the influence of board governance mechanisms on disclosure quality.	Ng and Yap (2022); Khadim and Kakar (2025); Parra and Rossi (2023)
P6	Proprietary cost concerns weaken the positive relationship between governance factors and cybersecurity risk disclosure (CRD) quality.	Even when firms have strong governance mechanisms, concerns over exposing sensitive cybersecurity information may constrain disclosure depth and reduce the effectiveness of governance in improving reporting quality.	Vo and Pham (2025); Jameel et al. (2025); Godewatta et al. (2025)

Table 2 shows that the proposed variables are theoretically grounded and are supported by emerging evidence from CRD literature, corporate governance and accounting studies. Governance mechanisms, including board's cybersecurity knowledge and board's independence, would contribute to stronger quality of CRD, whereas regulatory enforcement would represent the external pressure for better disclosure. In contrast, proprietary cost consideration would discourage a more extensive level of CRD. Moreover, the institutional variables in Malaysia, such as concentration of ownership, maturity of governance structure and reporting cultures, will affect how the governance mechanisms influence the disclosures.

Conclusion

This conceptual framework aims to explore the quality of cybersecurity risk disclosures (CRDs) in annual reports, considering the Malaysian emerging market. Drawing on signaling theory, proprietary cost theory, and corporate governance theory, this framework posits that board cybersecurity expertise, board independence, and strength of regulatory enforcement positively drive disclosure quality, whereas proprietary cost considerations act as a constraint, preventing detailed cybersecurity information disclosures. Further analysis of the model suggests that the institutional characteristics of Malaysia, such as concentration of ownership and heterogeneous governance maturity, can influence the impact of governance mechanism on CRD quality. These hypotheses are consistent with existing studies that highlight the

importance of governance quality and regulatory enforcement for cybersecurity transparency (Alodat et al., 2024; Smaili & Radu, 2023), whereas highlighting the constraining factors of proprietary costs (Vo & Pham, 2025).

This paper adds to accounting and accounting information systems literature by providing a comprehensive conceptual framework of CRD for the Malaysian emerging market by integrating research conducted across various disciplinary fields. As this research is of conceptual nature, future empirical testing of these propositions is recommended through annual reports content analysis, development of CRD indices or comparative study across various sectors and institutional settings in order to obtain further evidence.

Acknowledgements:	The authors would like to express their sincere gratitude to Faculty of Accountancy, Universiti Teknologi MARA Cawangan Kelantan, for providing the necessary resources and support throughout the course of this research. Special appreciation is extended to colleagues and peers who contributed valuable insights and constructive feedback, which greatly enhanced the quality of this paper.
Funding Statement:	No Funding
Conflict of Interest Statement:	The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the Advanced International Journal of Business, Entrepreneurship and SMEs (AIJBES).
Ethics Statement:	This study did not involve any human participants, animals, or sensitive data requiring ethical approval. The authors confirm that the research was conducted in accordance with accepted academic integrity and ethical publishing standards.
Author Contribution Statement:	All authors contributed significantly to the development of this manuscript. Ros Amalina Zakaria was responsible for the conceptualization, methodology, and overall supervision of the study. Azilawati Abdullah@Abd Aziz and Nor Asmawani Che Hassan contributed to the literature review and theoretical discussion, drafting, and critical revision of the manuscript. All authors read and approved the final version of the manuscript before submission.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 374-384

References

Alodat, A. Y., Hao, Y., Nobanee, H., Ali, H., Mansour, M., & Al Amosh, H. (2024). Board characteristics and cybersecurity disclosure: Evidence from UK listed firms. *Electronic Commerce Research*. https://doi.org/10.1007/s10660-024-09867-w

Block, M. (2025). Market reactions to material cybersecurity incident disclosures. *arXiv*. https://arxiv.org/abs/2512.06144

Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics, 187*(1), 199–224. https://doi.org/10.1007/s10551-022-05107-z

Deloitte. (2025). *Cybersecurity disclosure reporting trends under SEC requirements*. Deloitte Insights. https://www2.deloitte.com

Gauch, S., Smith, L., & Brown, T. (2025). Mandatory cybersecurity disclosure and investor reactions: Evidence from SEC filings. *International Journal of Accounting Information Systems, 57*, 100775. https://doi.org/10.1016/j.accinf.2025.100775

Godewatta, K., Wang, Y., & Lee, J. (2025). Cyber risk disclosure quality and market efficiency. *Journal of Financial Reporting and Accounting*. https://doi.org/10.1108/JFRA-2024-0123

Hagens Berman. (2025). *F5, Inc. faces investor scrutiny following cybersecurity incident*. Business Wire. https://www.businesswire.com/news/home/20251223511519/en/Hagens-Berman-Announces-Investigation-into-F5-Inc.-FFIV-Which-Faces-Securities-Class-Action-Amid-Cybersecurity-Incident-Questions-About-Disclosure-Timing-and-Impact-on-Companys-Business

Jameel, A., Khan, S., & Ahmed, R. (2025). Symbolic governance and cybersecurity disclosure quality. *Corporate Governance: An International Review*. https://doi.org/10.1111/corg.12567

Khadim, S., & Kakar, P. (2025). Board expertise and cybersecurity risk disclosure: Evidence from emerging markets. *Journal of Business Research, 158*, 113–128. https://doi.org/10.1016/j.jbusres.2024.113128

Moll, J., & Yigitbasioglu, O. (2025). The role of accounting in the digital age: AI, analytics, and automation. *Accounting, Auditing & Accountability Journal, 38*(2), 311–335. https://doi.org/10.1108/AAAJ-2023-0102

Ng, E. Y., & Yap, B. (2022). Digital transformation and governance challenges in Malaysian firms. *Asian Journal of Business and Accounting, 15*(2), 55–78.

Parra, M., & Rossi, F. (2023). Technostress in digital workplaces: A systematic review. *Information Systems Frontiers, 25*(3), 789–805. https://doi.org/10.1007/s10796-022-10345-2

Smaili, N., & Radu, C. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance, 27*, 1049–1071. https://doi.org/10.1007/s10997-022-09637-6

Sun, T., & Zhang, P. (2022). Artificial intelligence in accounting: Implications for professional roles. *Accounting Horizons, 36*(4), 45–60. https://doi.org/10.2308/HORIZONS-2021-015

U.S. Securities and Exchange Commission. (2024). *SEC guidance on cybersecurity disclosure*. https://www.sec.gov/news/press-release/2024-30

Vo, D. H., & Pham, T. H. (2025). Proprietary costs and voluntary disclosure decisions in cybersecurity reporting. *Journal of Accounting Research, 63*(1), 89–120. https://doi.org/10.1111/1475-679X.12456.