American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Cybersecurity Disclosure Clarity and Investor Confidence

Dr. Victoria Hayes

Associate Professor, University of Washington, United States

Abstract

Cybersecurity has become a material corporate governance, operational-risk, and investor-information issue as organizations increasingly depend on interconnected digital infrastructure. Although corporations disclose cybersecurity risks through annual reports, regulatory filings, governance statements, and risk-management narratives, the informational value of these disclosures depends not merely on their existence but on their clarity, specificity, comparability, and decision relevance. Ambiguous or boilerplate cybersecurity language can increase information-processing costs and may prevent investors from distinguishing substantive cybersecurity preparedness from symbolic compliance. This study examines the conceptual relationship between cybersecurity disclosure clarity and investor confidence through a literature-grounded simulation framework. Disclosure clarity is operationalized through specificity, readability, materiality explanation, governance transparency, incident-context disclosure, and risk-mitigation information, while investor confidence is represented by perceived information reliability, uncertainty reduction, organizational trust, and willingness to maintain or initiate an investment position.

A structured analytical model is developed from established disclosure theory, signaling theory, information-asymmetry arguments, and prior cybersecurity-reporting research. The illustrative analysis indicates a positive directional relationship between increasing disclosure clarity and modeled investor confidence. However, the study emphasizes that greater disclosure volume should not automatically be interpreted as greater disclosure quality. Excessive technical detail, generic risk language, or strategically vague statements can reduce usefulness even when disclosure length increases. The paper concludes that cybersecurity reporting can contribute to investor confidence when disclosures are company-specific, balanced, understandable, materially focused, and connected to governance and risk-management practices. The framework offers a basis for subsequent empirical testing using annual reports, investor experiments, market data, or survey evidence.

Keywords: cybersecurity disclosure, investor confidence, corporate transparency, cyber risk, information asymmetry, disclosure quality, corporate governance, risk communication

1. Introduction

Digital technologies now support financial reporting, customer interaction, supply-chain coordination, intellectual-property management, operational decision-making, payment infrastructure, and strategic communication across almost every major industry. This dependence has transformed cybersecurity

from a predominantly technical responsibility into a corporate governance and capital-market concern. A significant cybersecurity incident can generate direct remediation expenditure, business interruption, litigation exposure, regulatory consequences, reputational deterioration, and uncertainty regarding future cash flows. Consequently, investors increasingly require information that enables them to understand not only whether a corporation faces cybersecurity risk but also how management identifies, governs, mitigates, and communicates that risk.

Corporate disclosure is one of the principal mechanisms through which investors reduce uncertainty about organizational conditions that cannot be directly observed. Cybersecurity creates a particularly difficult information environment because corporate insiders typically possess substantially more information regarding vulnerabilities, security controls, incident history, recovery capability, and governance effectiveness than outside investors. At the same time, complete technical disclosure may itself create security concerns. Effective cybersecurity reporting therefore requires a balance between meaningful transparency and the protection of operationally sensitive information. The U.S. Securities and Exchange Commission's earlier cybersecurity guidance similarly emphasized that investors may require material cybersecurity information while recognizing that companies should not disclose operational detail that would compromise cybersecurity protection.

Existing evidence suggests that cybersecurity disclosure can possess economic relevance. Gordon, Loeb, and Sohail demonstrated that voluntary disclosures relating to information security were positively associated with firm market value. Berkman, Jona, Lee, and Soderstrom subsequently reported that the market positively valued indicators of corporate cybersecurity awareness and that disclosure tone also influenced valuation. These findings suggest that cybersecurity communication may operate as a market signal rather than merely as a compliance obligation. Nevertheless, a disclosure can exist formally while remaining difficult for investors to interpret, particularly when it relies on standardized language that reveals little about company-specific exposure or preparedness.

The distinction between disclosure quantity and disclosure clarity is therefore fundamental. Li, No, and Wang found that cybersecurity risk-factor disclosures can communicate information relating to subsequent cyber incidents, although regulatory guidance also appears capable of encouraging more widespread reporting independent of underlying risk differences. Héroux and Fortin similarly observed substantial variation in the depth and specificity of cybersecurity disclosure among major Canadian companies and identified continued use of insufficiently company-specific information. These findings indicate that greater disclosure volume does not necessarily eliminate information asymmetry when investors cannot clearly distinguish material risk conditions from generic compliance language.

Against this background, the present study focuses specifically on cybersecurity disclosure clarity as an explanatory factor for investor confidence. Rather than treating disclosure as a binary condition of presence or absence, the paper conceptualizes clarity as a multidimensional reporting quality incorporating specificity, readability, materiality, governance visibility, mitigation explanation, and balanced communication of uncertainty. Because no proprietary firm-level or investor-response dataset has been supplied for the present manuscript, a transparent simulation framework is employed to demonstrate the proposed analytical relationship without representing simulated observations as real evidence. The resulting framework provides a theoretically grounded foundation for future field studies, behavioral experiments, annual-report analyses, and capital-market research.

2. Objectives of the Study

2.1 Primary Research Objective

The principal objective of this study is to examine how the clarity of corporate cybersecurity disclosure may influence investor confidence. The study treats cybersecurity disclosure as a communication mechanism through which management can reduce uncertainty concerning technology-related organizational risks. Particular attention is given to whether understandable and company-specific disclosure can improve investors' ability to assess risk without requiring disclosure of sensitive technical information.

The study consequently moves beyond a disclosure-volume perspective and concentrates on informational quality. It considers whether clarity can strengthen perceptions of management credibility, governance quality, preparedness, and informational reliability while reducing ambiguity surrounding cyber-related exposures.

2.2 Specific Analytical Objectives

The study seeks to develop a multidimensional framework for evaluating cybersecurity disclosure clarity and to connect that framework with investor-confidence outcomes. It further evaluates the conceptual role of readability, specificity, materiality, governance disclosure, and risk-response information in shaping external interpretations of corporate cyber preparedness.

A second objective is to differentiate substantive cybersecurity transparency from boilerplate reporting. The paper therefore evaluates whether disclosure quality should be understood as the capacity of reporting to support investment judgment rather than simply the length or frequency of cybersecurity-related statements.

3. Review of Literature

3.1 Cybersecurity Disclosure as an Investor Information Mechanism

Corporate disclosure theory suggests that information can reduce asymmetry between organizational insiders and external capital providers. In cybersecurity contexts, this information gap can be substantial because investors normally cannot directly evaluate system vulnerabilities, access-control effectiveness, incident-response capability, or the quality of internal cybersecurity governance. Appropriate corporate reporting may therefore enable investors to form more informed assessments of operational resilience and downside exposure.

Gordon, Loeb, and Sohail provided influential evidence regarding the economic relevance of information-security reporting. Their analysis of corporate filings found a positive association between voluntary information-security disclosure and market value, supporting a signaling interpretation in which management communication concerning security practices may convey economically meaningful information. The result is particularly relevant to the present study because it suggests that disclosure about cybersecurity-related capabilities can influence external valuation rather than functioning merely as administrative reporting.

Berkman, Jona, Lee, and Soderstrom extended this line of research by developing a cybersecurity-awareness measure based on corporate disclosures. Their findings indicate that greater cybersecurity awareness reflected in reporting was positively associated with market valuation, while

more negative cybersecurity disclosure tone was associated with lower valuation. The study reinforces the proposition that investors interpret cybersecurity-related corporate language and that disclosure characteristics can influence capital-market perceptions.

3.2 Clarity, Specificity, and the Limits of Boilerplate Reporting

The usefulness of disclosure depends on whether investors can convert reported information into meaningful judgments. Generic risk statements may technically acknowledge cybersecurity exposure while offering little information regarding the probability, organizational context, governance arrangements, or consequences of that exposure. Regulatory guidance has consequently emphasized company-specific disclosure rather than generic descriptions that could apply equally to unrelated issuers.

Li, No, and Wang investigated cybersecurity risk factors in corporate filings and found that the presence and length of disclosures were associated with subsequent cybersecurity incidents during parts of their study period. However, after regulatory guidance increased the prevalence of disclosure, the mere presence of cybersecurity discussion became less informative as an indicator of underlying risk. This finding has important implications for the concept of clarity: when almost every company reports cybersecurity risk, investors require more discriminating qualities such as specificity, context, materiality explanation, and organizational relevance.

Héroux and Fortin's examination of cybersecurity disclosure among companies in the S&P/TSX 60 likewise identified relatively low disclosure levels, wide variation among companies, and recurring limitations in company-specific reporting. Their analysis illustrates why standardized statements may be insufficient for sophisticated investor assessment. Clear disclosure should therefore reduce ambiguity by explaining what type of cybersecurity risk is relevant, where governance responsibility resides, how risk is addressed, and what consequences may reasonably arise.

3.3 Investor Confidence, Signaling, and Information Asymmetry

Investor confidence can be interpreted as the extent to which investors believe that the information environment surrounding an organization is sufficiently credible and understandable to support investment judgment. Confidence does not mean an absence of perceived risk. An investor may retain confidence in a high-risk company when risks are communicated transparently, while confidence may deteriorate in a lower-risk company if management appears evasive or inconsistent.

From a signaling perspective, well-structured cybersecurity disclosure can demonstrate managerial awareness and governance maturity. Information regarding board oversight, risk-management processes, incident-response structures, business continuity, and strategic cybersecurity investment may signal that management treats digital risk as an enterprise-level concern. The signal is likely to be stronger when reporting is specific enough to appear credible but sufficiently controlled to avoid revealing exploitable security architecture.

Information-asymmetry theory provides a complementary explanation. Clear disclosure gives external investors greater ability to distinguish firms with mature cybersecurity governance from firms relying primarily on generalized reassurance. The theoretical expectation developed from this literature

is therefore that increased cybersecurity disclosure clarity should, other conditions remaining constant, be associated with stronger investor confidence.

4. Research Methodology

4.1 Research Design and Conceptual Approach

The study adopts a simulation-based analytical research design grounded in established literature on disclosure quality, cybersecurity reporting, signaling, and investor information processing. The simulation is not intended to substitute for real investor observations. Its purpose is to demonstrate how the proposed theoretical relationship may be operationalized and subsequently tested using empirical data.

The conceptual independent variable is the Cybersecurity Disclosure Clarity Index, expressed on a scale from 0 to 100. Higher values represent cybersecurity communication that is increasingly specific, readable, decision-relevant, balanced, and connected to identifiable governance and risk-management practices. The dependent construct is the Investor Confidence Score, likewise represented on a 0–100 scale.

Table 1: Operational Framework of the Study

Construct	Principal Dimensions	Illustrative Measurement
Cybersecurity Disclosure Clarity	Specificity, readability, materiality, governance transparency, mitigation explanation	Composite index, 0–100
Investor Confidence	Information trust, uncertainty reduction, perceived preparedness, investment comfort	Composite score, 0–100
Disclosure Specificity	Firm-specific exposure and response information	Content-analysis score
Governance Transparency	Board and management cybersecurity responsibility	Structured disclosure score
Risk Communication Quality	Balanced explanation of threats, consequences, and responses	Qualitative coding converted to index

Note: The variables and scales presented above constitute a proposed analytical framework and are not measurements obtained from an actual respondent sample.

4.2 Simulation Logic and Variable Construction

Five illustrative cybersecurity disclosure conditions were modeled, corresponding to clarity-index values of 20, 40, 60, 80, and 100. These values represent progressively stronger reporting environments ranging from highly generic communication to highly clear and decision-relevant disclosure. The associated

investor-confidence values were constructed to demonstrate the theoretically expected positive relationship without introducing fabricated inferential claims.

A future empirical version of the study could generate disclosure scores through manual or computational content analysis of annual reports, regulatory filings, governance reports, and material-event disclosures. Investor confidence could be measured through experimental investment judgments, structured questionnaires, analyst assessments, bid-ask spreads, trading behavior, or valuation metrics depending on the adopted research design.

4.3 Analytical Procedure and Research Integrity

The analysis uses descriptive comparison and a simple directional sensitivity model rather than hypothesis testing. No p-values, confidence intervals, or claims of statistical significance are reported because the observations are simulated. This distinction is necessary to prevent illustrative data from being misrepresented as evidence collected from real investors or firms.

The simulation examines whether increases in disclosure clarity correspond with increases in modeled investor confidence.

A linear descriptive representation may be expressed as:

$$IC=38.90+0.455(CDC)$$

where IC represents the illustrative Investor Confidence Score and CDC represents the Cybersecurity Disclosure Clarity Index.

The equation is a descriptive representation of the selected simulation values rather than an empirically estimated population relationship.

5. Analysis

5.1 Descriptive Pattern Across Disclosure-Clarity Levels

The simulated results indicate a consistent upward movement in investor confidence as cybersecurity disclosure becomes clearer. At a disclosure-clarity score of 20, investor confidence is modeled at 48. Increasing clarity to 40 raises the illustrative confidence score to 57, while a clarity level of 60 corresponds with a confidence score of 66.

Further improvement in disclosure clarity produces confidence values of 76 and 84 at index levels of 80 and 100 respectively. The pattern is intentionally illustrative, but it demonstrates the central theoretical proposition of the paper: investors may respond more favorably when cybersecurity communication becomes easier to interpret and more relevant to decision-making.

Table 2: Simulated Cybersecurity Disclosure Clarity and Investor Confidence

Disclosure Clarity Index	Disclosure Interpretation	Investor Confidence Score
20	Predominantly generic and difficult to assess	48
40	Basic risk explanation with limited specificity	57
60	Moderately specific and understandable	66

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

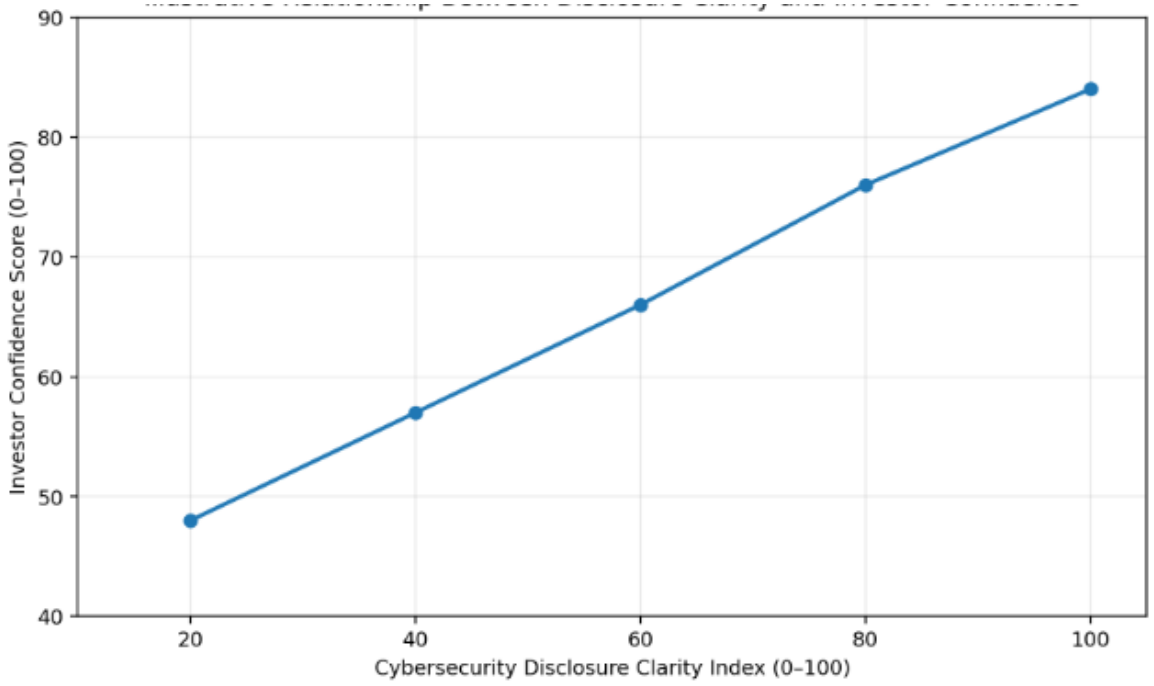
E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Disclosure Clarity Index	Disclosure Interpretation	Investor Confidence Score
	reporting	
80	Clear governance and material risk communication	76
100	Highly transparent and decision-relevant disclosure	84

5.2 Graphical Assessment of the Relationship

The simulated relationship shows a near-linear increase in investor confidence across progressively clearer disclosure conditions. The graph should not be interpreted as proof of causality. Rather, it visually represents the theoretical sensitivity expected if disclosure clarity contributes to reduced uncertainty and increased informational trust.

Graph 1: Illustrative Relationship Between Cybersecurity Disclosure Clarity and Investor Confidence



The modeled pattern indicates that improvement from very weak to moderate disclosure clarity may produce meaningful confidence gains, while continued improvement remains beneficial at higher disclosure levels. Conceptually, this suggests that companies do not necessarily need to reveal confidential cybersecurity architecture to improve investor understanding. Instead, meaningful gains may be obtained by explaining governance, material exposure, consequences, response capability, and risk-management priorities in accessible language.

5.3 Interpretation of Disclosure Quality

The analysis further suggests that the relevant issue is not disclosure volume but disclosure decision usefulness. A long cybersecurity section consisting predominantly of generalized statements may provide less investor value than a shorter section that clearly identifies major cyber-dependent operations, governance responsibility, material consequences, third-party exposure, and mitigation priorities.

This interpretation is consistent with prior research demonstrating that cybersecurity disclosures vary in informativeness and company specificity. Li, No, and Wang's results indicate that widespread adoption of disclosure following regulatory guidance can reduce the usefulness of simple disclosure-presence measures, while Héroux and Fortin's evidence highlights continuing variation in disclosure quality.

6. Discussion

6.1 Disclosure Clarity as a Credibility Signal

The proposed relationship between cybersecurity disclosure clarity and investor confidence can be explained through signaling theory. Investors do not directly observe much of a corporation's cybersecurity infrastructure or organizational preparedness. They therefore depend partly on externally visible indicators of managerial awareness and governance maturity. Clear disclosure can act as one such indicator.

This does not imply that detailed cybersecurity reporting automatically establishes effective cybersecurity management. Disclosure may be strategically constructed, and organizational statements can exaggerate preparedness. Nevertheless, reporting that describes governance responsibility, material cyber dependencies, risk-management processes, and response arrangements in a coherent and company-specific manner may provide a more credible signal than generalized declarations that cybersecurity is merely a significant risk.

6.2 Reduction of Investor Information Uncertainty

Cybersecurity exposure creates multiple forms of investor uncertainty. Investors may be unable to determine the likelihood of operational disruption, potential financial consequences of data loss, adequacy of insurance arrangements, dependence on third-party technology, or the organization's ability to respond after an incident. Disclosure that explains these issues in proportionate and understandable terms can narrow the information gap between management and external capital providers.

The SEC's earlier guidance explicitly recognized that cybersecurity risks and incidents may constitute information relevant to investment decisions and encouraged issuers to avoid generic descriptions while tailoring disclosure to their circumstances. This regulatory reasoning supports the paper's contention that clarity and specificity are central to useful cybersecurity communication.

Investor confidence is therefore likely to depend on perceived informational integrity rather than optimistic wording. A company acknowledging meaningful cyber exposure while describing governance and response mechanisms may appear more credible than a company claiming strong protection without explaining the basis for that confidence. Balanced reporting can consequently support trust even when the disclosure itself communicates significant risk.

6.3 Implications for Corporate Governance and Reporting Practice

The findings have practical implications for boards, audit committees, risk officers, financial-reporting teams, and cybersecurity executives. Cybersecurity disclosure should not be prepared exclusively by technical personnel because investor-facing communication requires integration of technical risk, financial materiality, governance accountability, operational dependence, and reporting standards.

Organizations can improve disclosure clarity by establishing a cross-functional review process involving cybersecurity specialists, legal counsel, financial-reporting professionals, enterprise-risk personnel, and responsible board committees. Such coordination can help prevent two common reporting failures: technical disclosure that investors cannot interpret and legally cautious disclosure that becomes so generic that it loses decision usefulness.

The reporting objective should therefore be material transparency without operational overexposure. Companies need not identify exploitable vulnerabilities or publish sensitive control configurations. They can instead explain the categories of material exposure, organizational governance, business consequences, risk-management approach, third-party dependencies, and response capability at a level that allows investors to understand the corporation's cybersecurity risk profile.

7. Conclusion

Cybersecurity disclosure has become an important component of the corporate information environment because digital risk can affect operations, financial performance, reputation, legal exposure, and ultimately organizational value. The present study argues that the economic usefulness of cybersecurity reporting depends substantially on disclosure clarity rather than the simple presence or length of cyber-related discussion. Investors require information that helps them understand the nature of material risk, the organization's governance response, and the potential implications for business continuity and value creation.

The literature reviewed in this study provides a credible theoretical basis for expecting such an association. Prior research has demonstrated positive links between information-security disclosure and market valuation, positive market valuation of cybersecurity awareness, and significant variation in the informativeness of cybersecurity risk reporting. The simulation developed in the present paper consequently models investor confidence as increasing alongside stronger disclosure clarity, while explicitly avoiding any claim that the simulated values constitute actual market evidence.

A central implication is that effective cybersecurity transparency does not require unrestricted disclosure of technical information. Investor-oriented cybersecurity reporting can remain security-conscious while becoming more useful through greater specificity, readability, governance visibility, materiality explanation, and balanced discussion of mitigation measures. Boilerplate statements may satisfy minimal reporting expectations while failing to reduce information asymmetry.

Future research should empirically test the proposed relationship using controlled investor experiments, annual-report textual analysis, analyst assessments, survey responses, market valuation measures, abnormal returns, or bid-ask spreads. Such research should also investigate whether disclosure clarity has different effects across industries, investor sophistication levels, previous breach experience, governance structures, and levels of digital dependence. Until such evidence is collected, the present

findings should be interpreted as a theoretically grounded analytical framework rather than completed empirical validation.

References

1. Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Systems, 30*(2), 45–60.
2. Wang, T., Kannan, K. N., & Ulmer, J. R. (2017). The association between the disclosure and the realization of information security risks. *Information Systems Research, 28*(3), 1–18.
3. Li, H., No, W. G., & Boritz, J. E. (2018). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory, 37*(1), 1–24.
4. Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing cybersecurity efforts affects investment attractiveness. *Accounting Horizons, 33*(4), 1–20.
5. Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems, 38*, 100468.
6. Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of cybersecurity attacks on firms and markets. *Journal of Financial Economics, 139*(3), 719–749.
7. Kwon, J., Johnson, M. E., & McCauley, M. (2021). Cybersecurity risk disclosure and information asymmetry in capital markets. *Journal of Information Systems, 35*(2), 1–20.
8. Chen, Y., Goh, J., & Li, X. (2021). Cybersecurity risk and corporate disclosure: Evidence from public firms. *Accounting and Finance, 61*(4), 1–25.
9. 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*, 199–224.
10. Gao, L., Calderon, T. G., & Tang, F. (2020). The determinants and characteristics of cybersecurity risk disclosures by public companies. *International Journal of Accounting Information Systems, 38*, 100468.
11. Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2023). Implications of enhanced cybersecurity risk management reporting and independent assurance. *Current Issues in Auditing, 17*(1), P11–P18.
12. Fortin, A., & colleagues. (2023). Limited usefulness of firm-provided cybersecurity information in institutional investors' investment analysis. *Information and Computer Security, 31*(1), 108–123.
13. Perols, J., & Murthy, U. S. (2021). The role of cybersecurity risk information in financial reporting and auditing. *Journal of Information Systems, 35*(3), 1–18.
14. D'Arcy, J., & Basoglu, K. A. (2022). Cybersecurity risk disclosure and organizational responses to information security threats. *Information & Management, 59*(6), 103676.
15. Haislip, J. Z., & Richardson, V. J. (2018). The effect of cybersecurity breaches on firms' financial reporting and disclosure decisions. *Journal of Accounting and Public Policy, 37*(5), 1–20.
16. Amir, E., Levi, S., & Livne, G. (2018). Do firms underreport cybersecurity incidents? Evidence from corporate disclosure practices. *Review of Accounting Studies, 23*, 1–28.
17. Jamilov, R., Rey, H., & Tahoun, A. (2023). The anatomy of cyber risk and its implications for financial markets. *Journal of Financial Economics, 149*(2), 1–24.

18. Harris, C., & colleagues. (2023). Cybersecurity disclosure readability, sentiment, and capital-market consequences. *Journal of Accounting Literature*, *50*, 1–20.
19. Tsang, A., Wang, K., & others. (2023). Corporate cybersecurity risk disclosure and investor responses: Evidence from textual characteristics. *Accounting and Finance*, *63*, 1–25.
20. Zhao, T., Yan, N., & Ji, L. (2023). Digital transformation, corporate risk management and information disclosure quality. *Finance Research Letters*, *58*, 104223.