

ECONOMY

Beyond Compliance: A Literature Review of Cybersecurity Disclosure, Corporate Governance, and Stakeholder Trust

Adli Rikanda Saputra^{1*}, Suherni Dwi Listiani², and Ridwansyah³

^{1,2}*Department of Sharia Accounting, Faculty of Islamic Economics and Business, Universitas Islam Negeri Raden Intan Lampung, Bandar Lampung, Indonesia*

³*Department of Sharia Banking, Faculty of Islamic Economics and Business, Universitas Islam Negeri Raden Intan Lampung, Bandar Lampung, Indonesia*

**Corresponding author: [adlirikandas@radenintan.ac.id]*

ABSTRACT

This study develops an integrated explanation of cybersecurity disclosure by synthesizing accounting, governance, finance, and information-systems research published between 2019 and 2026. A structured integrative literature review was applied to a curated corpus of 44 publications, identified through searches of Scopus and Google Scholar and screened against topical-relevance criteria. The studies were coded according to disclosure type, measurement attributes, governance and institutional determinants, stakeholder group, outcome, and contextual condition. The evidence shows that cybersecurity reporting includes risk, governance, preventive, incident, and mitigative information, which should not be treated as interchangeable constructs. Board independence, information technology expertise, dedicated cyber committees, gender diversity, internal controls, breach history, regulation, and sectoral exposure shape the extent and content of reporting. Disclosure can reduce information asymmetry, strengthen reputation, support firm value, moderate breach contagion, and inform audit risk assessment. However, longer or more readable reporting does not necessarily indicate stronger preparedness and may reveal heightened cyber exposure, increase stock-price crash risk, or generate adversarial costs. Boilerplate language, delayed incident reporting, strategic news timing, and possible manipulation of incident discovery dates further weaken credibility. The review contributes a Cyber Transparency Security Trust framework in which governance capacity and cyber exposure shape disclosure attributes, stakeholders assess both usefulness and security sensitivity, and resulting responses affect market value, audit fees, reputation, trust, and future cyber risk. The review is limited by its curated rather than exhaustive corpus and its focus on predominantly listed firms in developed economies. Future research should prioritize disclosure quality, preventive versus mitigative content, independent assurance, materiality judgments, emerging economies, artificial-intelligence-based analysis, and causal evidence on subsequent cyberattacks.

Keywords: *Cybersecurity Disclosure, Cyber Risk, Corporate Governance, Corporate Reporting, Information Asymmetry.*

1. INTRODUCTION

Cybersecurity risk has moved beyond the boundaries of information-technology departments and become a material governance and reporting concern. Digital business models depend on customer data, cloud infrastructure, payment platforms, software vendors, and interconnected supply chains. A cyber incident can therefore interrupt operations, compromise

confidential information, trigger regulatory action, damage stakeholder relationships, and reduce firm value. Corporate reporting is expected to explain how such risks are governed and managed, yet the technical complexity of cybersecurity leaves outside stakeholders dependent on information selected and framed by management (Amosh & Khatib, 2024; Cortez & Dekker, 2022; Haapamäki & Sihvonen, 2019).

Cybersecurity disclosure is not a single construct. Cyber-risk disclosure describes prospective exposure and material vulnerabilities; governance disclosure identifies board responsibilities, expertise, policies, and oversight structures; preventive disclosure communicates preparedness and risk-reduction measures; incident disclosure reports an event and its consequences; and mitigative disclosure explains containment, recovery, and remediation. Studies that combine these categories can reach different conclusions because proactive preparedness, generic risk language, and post-breach communication convey different information to investors, auditors, customers, regulators, and potential attackers.

The central challenge is a transparency-security paradox. More specific information can reduce information asymmetry, signal preparedness, and facilitate stakeholder monitoring. However, excessive technical detail may expose weaknesses, attract adversarial attention, or increase the probability of subsequent attacks (Magnan & Moldovan, 2025). The same reporting practice can also have different meanings. Extensive disclosure may indicate strong governance, elevated risk, regulatory pressure, or impression management. Cao et al. (2026), for example, show that preventive strategies can attenuate market losses following a breach, whereas mitigative descriptions may amplify negative reactions because they confirm the severity of the event.

Empirical evidence remains heterogeneous. Cybersecurity reporting is associated with firm performance and reputation in some settings, yet disclosure frequency has also been linked to stock-price crash risk (Amosh & Khatib, 2024; Singh, 2024; Wu et al., 2024). Readability can lower audit fees, while easy-to-read disclosure may simultaneously increase adversarial exposure (Calderon & Gao, 2020; Magnan & Moldovan, 2025). Board independence, IT expertise, cyber committees, and female representation generally strengthen disclosure, but effects vary by critical mass, governance position, national culture, and regulatory system (Afroze et al., 2025; Kurnia & Ardianto, 2024). Analysts also report that generic, boilerplate statements provide little decision-useful information (Fortin & Héroux, 2022).

Existing research therefore requires integration beyond a simple inventory of disclosure determinants. The literature frequently treats disclosure volume, specificity, readability, governance reporting, incident communication, and actual cybersecurity capability as equivalent. This study addresses that fragmentation through a structured integrative review. It asks how theoretical mechanisms explain cybersecurity disclosure; how measurement choices shape empirical findings; how governance, regulation, and incidents determine reporting; how disclosure affects different stakeholders; and when transparency builds trust without imposing

excessive security costs. The contribution is a Cyber Transparency Security Trust framework that connects organizational capacity and cyber exposure to disclosure attributes, credibility assessment, stakeholder responses, and economic or relational outcomes

. Prior systematic reviews on corporate cybersecurity have either focused broadly on the general determinants and consequences of cybersecurity risk across disciplines (Liu & Babar, 2024) or examined governance determinants of disclosure without distinguishing disclosure into distinct types, leaving unclear how risk, governance, preventive, incident, and mitigative disclosure differ in their stakeholder implications. Moreover, existing reviews do not explicitly model the transparency-security paradox as a structural mechanism linking governance capacity to disclosure outcomes. This study addresses these gaps by systematically differentiating disclosure into five distinct types, extending literature coverage to 2019–2026, and proposing the Cyber Transparency Security Trust (CTST) framework, which explicitly links governance capacity and cyber exposure to disclosure attributes, stakeholder credibility, and economic outcomes.

2. METHODS

2.1. Research Design and Review Scope

The study employs a structured integrative literature review. This design is suitable because cybersecurity disclosure research spans archival panel studies, event studies, experiments, interviews, content analysis, textual analysis, machine-learning applications, regulatory research, and systematic reviews. An integrative design permits these heterogeneous forms of evidence to be compared through common constructs and mechanisms. The review is structured because the corpus, eligibility criteria, coding dimensions, and synthesis procedure are specified. It is not presented as an exhaustive PRISMA-based systematic review because the available source corpus was curated for this article and does not contain a complete record of database searches, duplicate removal, and sequential screening.

The initial corpus comprises 44 publications dated from 2019 to 2026. It includes direct studies of cybersecurity-risk, governance, incident, preventive, and mitigative disclosure; research on board structure, IT expertise, gender diversity, regulation, assurance, and internal controls; and studies of consequences for markets, auditors, customers, reputation, and future attacks. Review articles were retained to establish the field's broader structure, but findings cited only through a secondary source were not treated as independent primary evidence. Sources were identified through searches of Scopus and Google Scholar; the initial search returned 50 records, of which 6 were excluded for lacking topical relevance, yielding the final curated corpus of 44 publications.

2.2. Eligibility Criteria and Evidence Classification

A publication was eligible when cybersecurity disclosure or cyber-incident reporting was a central construct; the study measured disclosure presence, extent, specificity, volume,

readability, tone, timeliness, or assurance; it examined governance, firm, incident, institutional, or regulatory determinants; or it assessed outcomes for a defined stakeholder. Studies concerned only with cybersecurity capability or sustainability performance were used as contextual evidence only when a direct disclosure mechanism was specified. Sources not used in the final synthesis were excluded from the reference list.

The evidence was classified into five analytical domains: conceptual and theoretical foundations; measurement and disclosure quality; organizational, governance, and institutional determinants; stakeholder and economic consequences; and emerging issues involving assurance, manipulation, artificial intelligence, ESG integration, and adversarial costs. Multiple classification was permitted because a study could simultaneously examine governance, textual properties, and market consequences.

Table 1. Review protocol and analytical dimensions

Stage	Procedure	Analytical Output
Corpus definition	Curated set of 44 publications from 2019-2026 concerning cyber-risk, governance, incident, preventive, mitigative, and assurance disclosure.	Transparent scope and methodological boundary.
Eligibility assessment	Direct evidence required an identifiable disclosure construct, determinant, stakeholder, outcome, or methodological contribution.	Separation of primary cyber-disclosure evidence from adjacent cybersecurity research.
Data extraction	Country, sector, period, disclosure type, measure, design, determinant, stakeholder, outcome, and main qualification.	Study-level analytical matrix.
Synthesis	Conceptual classification, attribute coding, mechanism-based comparison, and integration of contradictory findings.	Cyber Transparency-Security-Trust framework and research agenda.

2.3. Data Extraction and Analytical Procedure

Each publication was coded for geographical and sectoral setting, observation period, disclosure type, measurement method, research design, determinant, stakeholder group, outcome, direction of association, and contextual qualification. The coding distinguished risk from incident disclosure; pre-breach from post-breach communication; preventive from mitigative content; quantity from quality; and disclosure from operational cybersecurity

capability. Textual attributes were recorded separately, including specificity, readability, numerical content, uncertainty, litigious language, tone, and timeliness.

The analysis proceeded in four stages. First, descriptive mapping identified the theories, countries, industries, methods, and stakeholder groups represented in the corpus. Second, conceptual coding separated disclosure forms and attributes. Third, thematic synthesis compared information, legitimacy, capability, and adversarial-cost mechanisms. Fourth, conflicting findings were interpreted across breach status, reporting content, regulation, governance system, sector, and national context. This procedure avoids simple vote counting and treats heterogeneity as evidence about boundary conditions.

2.4. Reliability and Methodological Boundaries

Four safeguards were used to strengthen analytical reliability. First, the review does not equate extensive reporting with high-quality reporting or strong cybersecurity preparedness. Second, associations are not interpreted as causal unless the underlying design supports such inference. Third, negative, insignificant, and mixed findings are retained. Fourth, conclusions described as recurrent are supported by several studies or by broad review evidence. Secondary citations are identified as such and are not listed as separate primary references.

The study has limitations. The curated corpus is not exhaustive, recent publications are overrepresented because the field is young, and measures vary substantially across studies. Developed economies and listed firms dominate the evidence. Some indices reward word frequency rather than decision usefulness, and confidential operational controls cannot be observed from public reports. The synthesis therefore identifies mechanisms and conditions rather than universal coefficient signs.

3. RESULTS AND DISCUSSIONS

3.1. Conceptual Architecture and Theoretical Mechanisms

The synthesis identifies five related but distinct forms of reporting. Cyber-risk disclosure communicates prospective exposure and uncertainty. Governance disclosure describes board oversight, responsibility, expertise, policy, and committee structures. Preventive disclosure concerns preparation, controls, training, detection, and resilience before an event. Incident disclosure communicates the occurrence, nature, materiality, and consequences of a breach. Mitigative disclosure describes containment, recovery, remediation, and stakeholder protection after the event. Treating all five as a single disclosure score can obscure whether a firm is signalling preparedness, acknowledging risk, complying with regulation, or restoring legitimacy.

Agency theory explains disclosure as a mechanism for reducing the information advantage of managers over shareholders. Cyber risk intensifies agency problems because technical complexity and uncertain losses make managerial effort difficult to evaluate (Cortez & Dekker,

2022). Stakeholder theory extends accountability to customers, employees, suppliers, and regulators whose data and operations may be affected (Amosh & Khatib, 2024; Ramírez et al., 2022). Signalling theory predicts that prepared firms communicate preventive strategies to distinguish themselves, while legitimacy theory explains increased reporting after breaches and public pressure (Cao et al., 2026; D'Arcy & Basoglu, 2022; Singh, 2024).

The resource-based view adds a capability mechanism. Boards with IT expertise, cyber committees, and organizational policies possess knowledge and structures that improve the capacity to produce forward-looking information (Afroze et al., 2025). These theories are complementary but incomplete without adversarial information costs. Disclosure can benefit legitimate users while giving potential attackers clues about systems, dependencies, or weaknesses. Cybersecurity reporting is therefore an optimization problem: the firm must provide material and credible information without disclosing exploitable operational detail.

3.2. Measurement Architecture and Disclosure Quality

The literature uses disclosure indices, manual and automated content analysis, word frequency, scoring grids, readability measures, tone, numerical specificity, uncertainty language, litigious language, and event timeliness. Ramírez et al. (2022) construct a multidimensional index covering strategy, technical and organizational measures, and capacity building. Héroux and Fortin (2020) assess 40 regulator-based items, whereas Putter et al. (2026) distinguish disclosure presence, level, and volume. These measures answer different questions and should not be interpreted interchangeably.

Textual analysis expands scale but can weaken construct validity. A large number of cybersecurity terms may indicate detailed transparency, elevated exposure, regulatory caution, or repetitive boilerplate. Calderon and Gao (2020, 2021) show that language and readability matter for audit pricing and cross-listing comparisons. Gauch et al. (2025) find that European cybersecurity sections are complex while incident descriptions are comparatively clear and standardized, a pattern consistent with impression management. Cheong et al. (2020) demonstrate that factor analysis can recover distinct content categories that word counts alone would miss.

Quality requires company specificity, materiality, timeliness, consistency, quantification, forward-looking content, clear governance responsibility, and balanced discussion of prevention and response. Boilerplate statements can satisfy formal expectations while remaining unhelpful to analysts (Fortin & Héroux, 2022). Lunga and Kirsten (2026) likewise find that firms often emphasize governance but provide limited information about impacts and mitigation. The synthesis therefore distinguishes disclosure volume from decision usefulness and treats readability as one attribute rather than a complete quality measure.

3.3. Corporate Governance and Organizational Capability

Board characteristics are recurrent determinants of cybersecurity disclosure. Board independence is positively associated with reporting in the Bangladeshi banking industry, supporting the monitoring explanation (Mazumder & Hossain, 2022). Board size can add expertise and stakeholder representation, and Afroze et al. (2025) find a positive association among FTSE 100 firms. Ereddia (2026) reports that board size, independence, IT expertise, and busy directors are positively associated with governance-over-cyber-risk disclosure, whereas longer-serving directors disclose less. These findings suggest that knowledge diversity and external orientation may be more important than formal board size alone.

Dedicated governance resources strengthen reporting capacity. Afroze et al. (2025) find that cyber committees and IT expertise are associated with more forward-looking disclosure. Elmarzouky et al. (2025) similarly show that board commitment - measured through IT expertise, committees, and cybersecurity policies - increases disclosure among UK firms. Kurair and Adedokun (2026) find that board IT expertise strengthens the relationship between cybersecurity and sustainability performance. Governance structures create value when they provide relevant competence, information access, and oversight authority, not merely when a committee exists on paper.

Internal controls and incident experience also shape reporting. Jiang et al. (2021) show that breached firms do not respond uniformly; prior experience and market reactions affect subsequent disclosure. Lin and She (2025) find that possible manipulation of incident discovery dates is more prevalent where internal controls are weak and litigation risk is low. These results connect governance capacity with disclosure integrity: firms need systems that identify, escalate, document, and assess incidents before the board can communicate them credibly.

3.4. Gender Diversity, Position, and Critical Mass

Gender diversity generally supports cyber transparency, but its effect depends on representation and governance position. Elnahass et al. (2024) find that female executives disclose more cybersecurity information and use a more conservative, uncertain, and litigious tone. Mazumder and Hossain (2022) report a positive association between female directors and disclosure in Bangladesh. Afroze et al. (2025), however, find no significant overall effect until boards have three or more female directors, supporting a critical-mass rather than token-representation explanation.

Kurnia and Ardianto (2024) provide important evidence from Indonesia's two-tier system. Women commissioners increase disclosure, while women on the management board are negatively associated with it. The authors relate the result to governance roles and patriarchal culture. The synthesis indicates that gender diversity should not be measured only as a single proportion. Future models should distinguish supervisory and executive roles, committee membership, IT experience, tenure, and critical mass.

3.5. Firm, Incident, Regulatory, and Institutional Determinants

Firm characteristics affect both cyber exposure and reporting resources. Singh (2025) identifies size, leverage, beta, and knowledge-intensive industry membership as determinants of voluntary disclosure in India. Financial constraints can increase exposure and alter cyber-risk language, as shown in the context of terrorism intensity by Phan et al. (2025). Sector is particularly important because financial, health, technology, and retail firms hold different data, face different regulations, and depend on digital infrastructure to different degrees.

Breach history creates public and institutional pressure. D'Arcy and Basoglu (2022) show that firms respond to their own breaches and the breaches of peers, but communication varies according to whether the source is internal or external. Chen et al. (2022) find that breached firms generally increase risk-factor disclosure and that decreasing disclosure after a breach triggers a negative market response. Reporting after an incident therefore reflects both new information and stakeholder expectations about how a responsible firm should respond.

Regulation increases reporting but does not automatically ensure quality. Elmarzouky et al. (2025) find that the UK NIS regulation strengthens the relationship between board commitment and disclosure. Gider et al. (2026) document a fragmented landscape across the United States and European Union, with different materiality, timing, privacy, and enforcement regimes. Regulation can standardize minimum content and timing, but boilerplate, inconsistent materiality judgments, and overlapping legal requirements remain. Assurance and internal control are therefore necessary complements to formal rules.

3.6. Credibility, Timeliness, Assurance, and Information Manipulation

Timeliness is central to incident disclosure because delayed information permits informed parties to trade or allows losses to remain hidden. Yet the date used to evaluate timeliness may itself be endogenous. Lin and She (2025) provide suggestive evidence that some firms influence the reported discovery date, supported by a spike in insider sales before that date. Kelton (2021) also documents widespread underreporting of incidents. A credible regime must therefore connect disclosure deadlines to documented internal escalation, forensic evidence, and audit trails rather than relying solely on management's reported date.

Firms may also manage attention. Magnan and Moldovan (2025) summarize evidence that busy news days can mute market reactions to breach announcements. Standardized or optimistic framing can reduce scrutiny even when the technical facts are disclosed. Credibility depends on consistency between risk factors, governance claims, incident details, remediation, and subsequent outcomes. A report that describes strong controls but repeatedly experiences similar breaches should be evaluated differently from a report supported by observable improvements.

Independent assurance can increase confidence, particularly after a prior attack. Frank et al. (2019) find that the benefit of cyber-risk-management reporting and assurance depends on

whether the firm has disclosed a previous attack. Navarro and Sutton (2025) show that industry expectations influence nonprofessional investors' judgments about voluntary assurance. Assurance is not a substitute for management responsibility, but it can improve confidence in governance processes, control descriptions, and the completeness of reported events. The field still lacks generally accepted assurance criteria and a consistent definition of cyber materiality.

Table 2. Interpretation of cybersecurity disclosure attributes

Attribute	Potential Benefit	Interpretive Risk	Preferred Evaluation
Volume	Signals attention and reporting effort.	May reflect elevated exposure or repeated boilerplate.	Assess specificity, balance, and year-to-year change.
Readability	Improves stakeholder access and can lower audit uncertainty.	May simplify severe events or reveal exploitable detail.	Combine with materiality, accuracy, and security sensitivity.
Timeliness	Reduces information asymmetry after an incident.	Reported discovery date may be delayed or manipulated.	Use documented detection, escalation, and forensic timelines.
Preventive content	Signals preparedness and can attenuate breach losses.	May become unverifiable policy language.	Seek controls, responsibilities, testing, and assurance.
Mitigative content	Explains containment and recovery.	Can confirm incident severity and trigger negative reactions.	Evaluate response effectiveness and affected stakeholders.
Assurance	Improves confidence in processes and completeness.	Scope may be narrow and criteria inconsistent.	Disclose provider, criteria, scope, level, and limitations.

3.7. Market, Firm-Performance, and Financing Consequences

The economic consequences of disclosure depend on whether reporting communicates preparedness, reveals risk, or follows an incident. Amosh and Khatib (2024) find positive accounting- and market-based associations in Australia, while Khoifin and Huang (2025) document value relevance in Southeast Asia. Singh (2024) finds that voluntary reporting

supports corporate reputation. These results are consistent with information and signalling benefits, but they do not imply that more disclosure always causes better performance. Successful firms may possess both stronger controls and greater reporting resources.

Risk revelation can produce the opposite result. Wu et al. (2024) associate disclosure frequency with stock-price crash risk in China, suggesting that reporting may reveal accumulated risk or reflect delayed bad news. Cortez and Dekker (2022) summarize substantial event-window losses following cyberattacks. Magnan and Moldovan (2025) show that market reaction can be influenced by the timing and surrounding news environment. Interpretation should therefore distinguish pre-breach risk disclosure from the announcement of realized losses.

Content is consequential. Cao et al. (2026) find that preventive strategies reduce market losses after a breach, whereas mitigative strategies amplify the negative effect. Preventive disclosure can indicate that a firm anticipated risk and invested in preparedness. Mitigative content may signal that the incident was severe enough to require extensive recovery. This distinction explains why apparently similar disclosures can generate opposite investor responses.

3.8. Auditor, Investor, Customer, and Supply-Chain Usefulness

Auditors incorporate cyber-risk information into risk assessment and pricing. Calderon and Gao (2020) find that disclosure content and language influence audit fees and that readability can reduce fees. Jiang (2024) reports that higher machine-learning-estimated cyber risk is associated with higher audit fees and that breach-related premiums depend on heightened underlying risk. Litt et al. (2023) show that a breach at a major audit firm can damage auditor reputation and alter client and shareholder behavior. Frank et al. (2026) find that auditors increasingly consider qualitative cybersecurity effects but remain uncertain about materiality judgments.

Investor usefulness is mixed. Individual investors indicate that incidents matter to their decisions, but institutional analysts often reject cursory reporting and rely on alternative information sources (Fortin & Héroux, 2022; Kelton, 2021). Information becomes useful when it is company-specific, material, timely, and connected to governance and operational consequences. Voluntary pre-breach disclosure also protects peer firms by attenuating contagion effects after an industry breach (Kelton & Pennington, 2019).

Cybersecurity transparency also matters in customer-supplier relationships. Nelson (2024) finds that major customers increase purchases from suppliers whose cybersecurity-awareness scores improve. Suppliers with weak security can transmit disruption and financial distress through the value chain. Stakeholder usefulness is therefore not uniform: auditors need control and materiality information, investors need financial exposure and governance, customers need

continuity and data-protection assurance, and regulators need timely, comparable incident information.

3.9. Reputation, Trust, and the Adversarial Cost of Transparency

Reputation and trust arise from consistency between claims, governance, preparedness, incident response, and subsequent outcomes. Singh (2024) finds that voluntary reporting is associated with stronger corporate reputation. Zhang (2024) shows that firms increase CSR engagement after data-breach disclosure laws and that CSR can provide reputational insurance around breaches. Yet symbolic communication can erode trust when firms emphasize policy statements without reporting impacts or remediation.

The adversarial-cost problem distinguishes cybersecurity from many other forms of disclosure. Longer or easier-to-read reports can help stakeholders but may reveal systems, dependencies, or security posture. Magnan and Moldovan (2025) report mixed evidence on disclosure length and subsequent attacks. The optimal report is therefore neither maximal secrecy nor unrestricted detail. It provides governance responsibilities, material risk, incident effects, resilience, and stakeholder protection while withholding operational instructions that could be exploited.

This balance can be represented as a two-dimensional assessment. High stakeholder usefulness with low adversarial exposure is credible transparency. High usefulness with high exposure requires careful aggregation and secure regulatory channels. Low usefulness with low exposure is boilerplate compliance. Low usefulness with high exposure is both uninformative and potentially harmful. This framework shifts evaluation from disclosure quantity toward purposeful, stakeholder-specific, and security-aware reporting.

3.10. Geographic and Sectoral Heterogeneity

Most evidence originates in the United States, Canada, the United Kingdom, Europe, and Australia. Canadian and South African studies report low and uneven quality despite growing disclosure (Héroux & Fortin, 2020; Lunga & Kirsten, 2026; Putter et al., 2026). Calderon and Gao (2021) find that foreign firms listed in the United States disclose more readable and numerically specific information than domestic firms. European firms use complex cyber sections but clearer standardized incident language (Gauch et al., 2025). These differences reflect regulation, litigation, reporting traditions, and managerial incentives.

Emerging-economy evidence shows both progress and distinctive governance conditions. Disclosure increased in Latin America, with financial firms reporting most extensively (Ramírez et al., 2022). Bangladesh, India, Indonesia, and South Africa reveal the importance of board structure, industry knowledge, culture, and resource constraints (Kurnia & Ardianto, 2024; Mazumder & Hossain, 2022; Singh, 2025). The financial sector is often the most active because it is data-intensive, highly regulated, and systemically exposed. Cross-sector indices should therefore adjust for different operational risks and stakeholder expectations.

3.11. Integrated Framework and Future Research Directions

Figure 1 integrates the review. Cyber exposure, breach history, governance capacity, internal controls, regulation, and stakeholder pressure shape reporting. Firms then choose disclosure attributes such as specificity, readability, tone, timeliness, preventive or mitigative orientation, and assurance. Stakeholders assess both credibility and security sensitivity. Investor, auditor, customer, regulator, and peer responses generate outcomes for market value, performance, fees, reputation, trust, and future cyber risk. These outcomes feed back into governance and subsequent reporting.

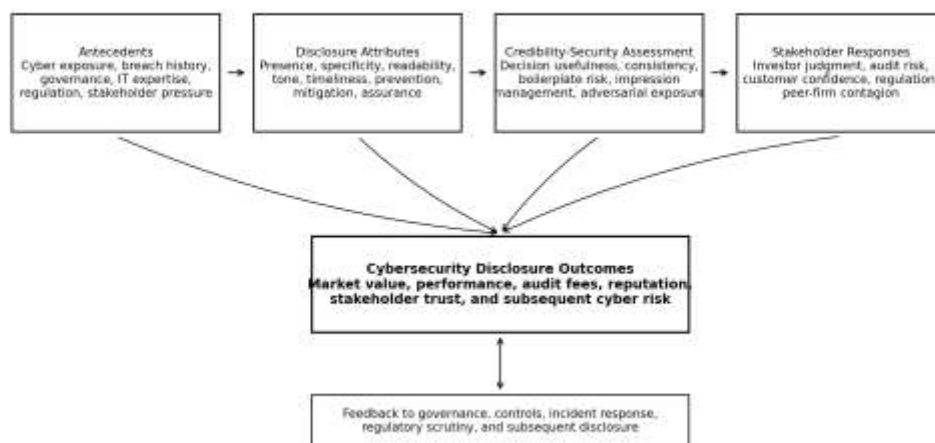


Figure 1. Cyber Transparency-Security-Trust framework

Future research should replace generic word counts with measures of materiality, company specificity, governance responsibility, and consistency across reporting channels. Preventive and mitigative communication should be tested separately, and researchers should examine whether managers substitute between delayed reporting, news bundling, and narrative framing. Incident timelines require validation through forensic and internal-control evidence. Studies of assurance should compare providers, criteria, scope, and stakeholder benefits.

More causal and longitudinal evidence is needed on whether disclosure changes cyber investment, incident frequency, loss severity, and stakeholder trust. Cross-country designs should compare materiality, privacy, litigation, and incident-reporting regimes. Emerging economies, smaller firms, supply chains, and Islamic financial institutions remain underexamined. Artificial intelligence and machine learning can improve classification, but models require transparent validation to avoid equating textual intensity with risk or preparedness. ESG integration should also preserve cybersecurity as a distinct governance and stakeholder-protection issue rather than burying it in an aggregate score.

4. CONCLUSION

This review shows that cybersecurity disclosure is a multidimensional governance practice rather than a single reporting quantity. Risk, governance, preventive, incident, and mitigative information address different stakeholder questions and can generate different market consequences. Disclosure volume, readability, and timeliness are relevant attributes, but none alone establishes credibility or operational preparedness. Company specificity, materiality, consistency, internal controls, assurance, and the relationship between reported policies and subsequent outcomes are equally important.

Corporate governance shapes reporting capacity. Board independence, IT expertise, dedicated cyber committees, gender diversity, and effective controls generally support more extensive or forward-looking communication, although effects vary across governance roles, critical mass, sectors, and national cultures. Regulation increases disclosure and can strengthen board commitment, but formal compliance does not automatically remove boilerplate language, inconsistent materiality judgments, or strategic timing. Independent assurance offers a promising credibility mechanism, particularly following a prior attack, yet common criteria remain underdeveloped.

Cybersecurity disclosure can reduce information asymmetry, support reputation, inform audit pricing, attenuate contagion, and strengthen customer relationships. It can also reveal severe exposure, increase crash risk, or create adversarial costs. Preventive information tends to signal preparedness, whereas mitigative reporting can confirm event severity. Effective policy should therefore seek optimal transparency: sufficient information for investors, auditors, customers, and regulators without disclosing exploitable operational detail.

The review is limited by a curated rather than exhaustive corpus, heterogeneous designs and measures, the dominance of listed firms and developed economies, and the absence of a new meta-analysis. Recent studies may also contain findings that have not yet accumulated extensive replication. The proposed framework should therefore be treated as an organizing explanation rather than a causal model. Its principal implication is that cybersecurity reporting should be evaluated through the combined lenses of transparency, credibility, stakeholder usefulness, and security sensitivity.

Future research could usefully pursue several specific directions. First, studies could develop and validate disclosure quality measures that distinguish preventive from mitigative content, rather than relying on aggregate disclosure volume or readability scores alone. Second, quasi-experimental designs such as difference in differences analyses around staggered adoption of mandatory disclosure regulations (e.g., the 2023 SEC cybersecurity disclosure rule) could help establish causal links between disclosure and outcomes such as audit fees or stock-price crash risk, addressing the correlational limitations of the current evidence base. Third, research could examine cybersecurity disclosure in small and medium-sized enterprises and in emerging-market firms, where governance structures and regulatory pressures differ

substantially from the listed, developed-economy firms that dominate current evidence. Fourth, studies could investigate the use of AI based textual analysis to detect boilerplate language, strategic timing of incident disclosure, and possible manipulation of breach discovery dates, moving beyond manual content coding. Finally, a future meta-analysis once a sufficient number of comparable effect sizes accumulate across the categories identified in this review could quantitatively synthesize the heterogeneous findings on governance determinants of disclosure.

5. REFERENCES

- Abdelraouf, M., & Hussainey, K. (2025). Systematic review of cyberrisk disclosure practices: Insights and implications. *The Journal of Risk Finance*. <https://doi.org/10.1108/JRF-07-2024-0210>
- Afroze, D., Ghosh, R., & Dey, P. K. (2025). Cybersecurity disclosure in the UK: The role of board attributes and female director critical mass. *Journal of Enterprise Information Management*, 39(4), 1309-1338. <https://doi.org/10.1108/JEIM-04-2025-0311>
- Amosh, H. A., & Khatib, S. F. A. (2024). Cybersecurity transparency and firm success: Insights from the Australian landscape. *Australian Economic Papers*, 64(2), 189-204. <https://doi.org/10.1111/1467-8454.12385>
- Calderon, T. G., & Gao, L. (2020). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing*, 25(1), 24-39. <https://doi.org/10.1111/ijau.12209>
- Calderon, T. G., & Gao, L. (2021). Comparing the cybersecurity risk disclosures of U.S. and foreign firms. *Journal of Emerging Technologies in Accounting*, 19(2), 61-79. <https://doi.org/10.2308/JETA-2020-008>
- Cao, R., Matta, M., Cavusoglu, H., Aziz, A., & Kafaee, O. (2026). Is prevention better than cure? Effects of cyber risk disclosures on shareholder response to breaches. *Information Systems Research*, 37(2), 842-862. <https://doi.org/10.1287/isre.2022.0405>
- Chen, J., Henry, E., & Jiang, X. (2022). 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>
- Cheong, A., Yoon, K., Cho, S., & No, W. G. (2020). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of Information Systems*, 35(2), 179-194. <https://doi.org/10.2308/ISYS-2020-031>
- Cortez, E. K., & Dekker, M. (2022). A corporate governance approach to cybersecurity risk disclosure. *European Journal of Risk Regulation*, 13(3), 443-463. <https://doi.org/10.1017/err.2022.10>
- D'Arcy, J., & Basoglu, A. (2022). The influences of public and institutional pressure on firms' cybersecurity disclosures. *Journal of the Association for Information Systems*, 23(3), 779-805. <https://doi.org/10.17705/1jais.00740>
- Eaton, T. V., Grenier, J. H., & Layman, D. M. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, 13(2), C1-C9. <https://doi.org/10.2308/ciia-52419>
- Elmarzouky, M., Moussa, T., & Allam, A. (2025). Cybersecurity disclosure: Board commitment and regulatory impact in the United Kingdom. *The International Journal of Accounting*. <https://doi.org/10.1142/S1094406025420053>

- Elnahass, M., Ahmed, Y., & Trinh, V. Q. (2024). Empowering women to lead cybersecurity: The effect of female executives on disclosure sentiment. *International Journal of Finance & Economics*, 30(4), 3368-3394. <https://doi.org/10.1002/ijfe.3067>
- Ereddia, L. E. (2026). Firm transparency of risk oversight: An examination of cybersecurity governance disclosures. *Journal of Information Systems*, 1-23. <https://doi.org/10.2308/ISYS-2024-012>
- Fortin, A., & Héroux, S. (2022). Limited usefulness of firm-provided cybersecurity information in institutional investors' investment analysis. *Information & Computer Security*, 31(1), 108-123. <https://doi.org/10.1108/ICS-07-2022-0122>
- Liu, C., & Babar, M. A. (2026). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management*, 51(1), 62-92.
- Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems*, 33(3), 183-200. <https://doi.org/10.2308/isys-52374>
- Frank, M., Grenier, J., Navarro, P., & Zhang, Y. (2026). Auditors' perceptions regarding cybersecurity and cybersecurity-related materiality. *Accounting Horizons*, 1-18. <https://doi.org/10.2308/HORIZONS-2023-094>
- Gauch, K., Schaffner, L. G., Behnam, E., & Prinz, E. (2025). European cybersecurity disclosure practices: A textual analysis. *International Journal of Disclosure and Governance*. <https://doi.org/10.1057/s41310-025-00327-x>
- Gider, J., Renneboog, L., & Strauss, T. (2026). The regulation of data privacy and cybersecurity. *Annals of Corporate Governance*, 10(1), 1-101. <https://doi.org/10.1108/ACG-07-2025-0050>
- Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, 34(7), 808-834. <https://doi.org/10.1108/MAJ-09-2018-2004>
- Héroux, S., & Fortin, A. (2020). Cybersecurity disclosure by the companies on the S&P/TSX 60 index. *Accounting Perspectives*, 19(2), 73-100. <https://doi.org/10.1111/1911-3838.12220>
- Jiang, W. (2024). Cybersecurity risk and audit pricing: A machine learning-based analysis. *Journal of Information Systems*, 38(1), 91-117. <https://doi.org/10.2308/ISYS-2023-019>
- Jiang, W., Legoria, J., Reichelt, K. J., & Walton, S. (2021). Firm use of cybersecurity risk disclosures. *Journal of Information Systems*, 36(1), 151-180. <https://doi.org/10.2308/ISYS-2020-067>
- Kelton, A. S. (2021). How to reduce the cybersecurity breach contagion effect. *Current Issues in Auditing*, 15(2), P1-P9. <https://doi.org/10.2308/CIIA-2020-025>
- Kelton, A. S., & Pennington, R. (2019). Do voluntary disclosures mitigate the cybersecurity breach contagion effect? *Journal of Information Systems*, 34(3), 133-157. <https://doi.org/10.2308/isys-52628>
- Khoifin, K., & Huang, Y. (2025). ESG and cybersecurity disclosure: Navigating corporate strategy through value relevance analysis. *Journal of Accounting & Organizational Change*, 1-32. <https://doi.org/10.1108/JAOC-03-2025-0070>
- Kurair, A. A. A., & Adedokun, M. W. (2026). Evaluating the influence of cybersecurity on sustainability performance: Role of digitalization intensity and board IT expertise in Frankfurt Stock Exchange firms. *Sustainable Development*. <https://doi.org/10.1002/sd.70816>

- Kurnia, P., & Ardianto, A. (2024). Board gender diversity and cyber security disclosure in the Indonesian banking industry: A two-tier governance context. *Corporate Governance: The International Journal of Business in Society*, 24(7), 1614-1637. <https://doi.org/10.1108/CG-01-2023-0010>
- Lin, X., & She, G. (2025). Timely cybersecurity disclosure and information manipulation. *Management Science*, 71(11), 9308-9327. <https://doi.org/10.1287/mnsc.2023.01058>
- Litt, B., Tanyi, P., & Watson, M. W. (2023). Cybersecurity breach at a Big 4 accounting firm: Effects on auditor reputation. *Journal of Information Systems*, 37(2), 77-100. <https://doi.org/10.2308/ISYS-2022-006>
- Liu, C., & Babar, M. A. (2024). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management*, 51(1), 62-92. <https://doi.org/10.1177/03128962241293658>
- Lunga, T., & Kirsten, E. (2026). Cybersecurity risk disclosure practices of Johannesburg Stock Exchange-listed companies. *International Journal of Disclosure and Governance*. <https://doi.org/10.1057/s41310-026-00389-5>
- Magnan, M., & Moldovan, R. (2025). Cybersecurity risks and incidents disclosure: A literature review. *Accounting Perspectives*, 24(3), 605-667. <https://doi.org/10.1111/1911-3838.12411>
- Mazumder, M. M. M., & Hossain, D. M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: Does board composition matter? *Journal of Accounting in Emerging Economies*, 13(2), 217-239. <https://doi.org/10.1108/JAEE-07-2021-0237>
- Navarro, P., & Sutton, S. G. (2025). Leveraging emerging cybersecurity reporting regulations: The effect of industry-driven expectations for voluntary assurance. *Accounting Horizons*, 39(1), 183-198. <https://doi.org/10.2308/HORIZONS-2023-088>
- Nelson, A. G. (2024). The importance of cybersecurity disclosures in customer relationships. *Journal of Corporate Accounting & Finance*, 35(3), 66-74. <https://doi.org/10.1002/jcaf.22695>
- Phan, A., Le, T. T. H., Truong, H. H. D., & Hoang, H. V. (2025). Skating on thin ice: Firm-level cybersecurity risk amid terrorist attacks. *Digital Policy, Regulation and Governance*, 28(2), 190-205. <https://doi.org/10.1108/DPRG-11-2024-0281>
- Putter, L. F., Johnson, R., & Mans-Kemp, N. (2026). Exploring cybersecurity disclosure in South Africa. *South African Journal of Economic and Management Sciences*, 29(1). <https://doi.org/10.4102/sajems.v29i1.6133>
- Ramírez, M., Ariza, L. R., Miranda, M. E. G., & Vartika, V. (2022). The disclosures of information on cybersecurity in listed companies in Latin America: Proposal for a cybersecurity disclosure index. *Sustainability*, 14(3), 1390. <https://doi.org/10.3390/su14031390>
- Singh, H. (2024). Is corporate reputation associated with voluntary cybersecurity risk reporting? *Meditari Accountancy Research*, 33(1), 198-219. <https://doi.org/10.1108/MEDAR-02-2024-2329>
- Singh, H. (2025). Voluntary cybersecurity risk disclosures and firms' characteristics: The moderating role of the knowledge-intensive industry. *Asian Journal of Accounting Research*, 10(2), 168-185. <https://doi.org/10.1108/AJAR-12-2023-0413>
- Walton, S., Wheeler, P., Zhang, Y., & Zhao, X. (2020). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems*, 35(1), 155-186. <https://doi.org/10.2308/ISYS-19-033>

- Wu, H., Ma, M., & Zhang, J. (2024). Impact of cybersecurity disclosure frequency on stock price crash risk. *Journal of Corporate Accounting & Finance*, 36(3), 87-102. <https://doi.org/10.1002/jcaf.22775>
- Zhang, Y. (2024). Data breach disclosure laws and social responsibility initiatives. *The International Journal of Accounting*, 60(4). <https://doi.org/10.1142/S1094406024400031>