

Cybersecurity Architecture and Esg Compliance: A Strategic Alignment Framework for Corporate Boards

Toluwase Itanola Ariyo

Subject Matter Expert, Kazian School of Management

Abstract—Cybersecurity risk and Environmental, Social, and Governance (ESG) performance have historically been governed as distinct corporate domains, with separate reporting lines, board committees, and performance measures. This paper examines the strategic rationale for aligning cybersecurity architecture — the technical, procedural, and organisational dimensions that secure information resources — with corporate boards' ESG compliance frameworks. Drawing on a structured literature and regulatory review (the SEC's 2023 cybersecurity disclosure rule, NIST Cybersecurity Framework 2.0, GRI, and SASB) together with an illustrative empirical analysis built from a simulated board-governance dataset (214 board/executive responses; 60 firms cross-sectionally) calibrated to patterns reported in published industry and academic sources, the paper finds a consistent positive relationship between cybersecurity architecture maturity and composite ESG performance (Pearson $r = 0.82$). Boards that formally embed cyber-risk oversight within governance and sustainability committees show greater risk-posture resilience, higher disclosure transparency, and stronger stakeholder trust than boards that keep the two functions separate. The paper introduces a conceptual alignment framework, ranks the governance barriers to integration, and closes with board-level recommendations, limitations, and a future research agenda linking cyber-ESG integration to firm valuation and cost of capital.

Index Terms—Cybersecurity Governance, ESG Compliance, Corporate Boards, Risk Oversight, NIST CSF 2.0, SEC Disclosure Rules, Sustainability Reporting

I. INTRODUCTION

Pressure is growing on corporate boards to demonstrate meaningful oversight of two previously distinct governance domains: cybersecurity risk and Environmental, Social and Governance (ESG) performance. Cybersecurity has traditionally

belonged to the Chief Information Security Officer (CISO) and the audit or risk committee, while sustainability has belonged to sustainability officers and, more recently, a board-level sustainability committee. This division is increasingly unworkable. Digital infrastructure now sits at the heart of nearly every facet of ESG performance: data privacy is a social issue, energy-efficient data-centre operations are an environmental issue, and the transparency, accountability and resilience of the systems that safeguard stakeholder data are, at their core, governance issues.

Regulators are beginning to codify this convergence. In July 2023 the U.S. Securities and Exchange Commission (SEC) issued final rules requiring public companies to disclose material cybersecurity incidents within four business days and to describe, in annual reports, how the board oversees cybersecurity risk and how management assesses and manages it (U.S. Securities and Exchange Commission, 2023; Deloitte, 2023). The rule is explicit about governance: companies must disclose which board committee oversees cyber risk and how that committee is kept informed (Sophos News, 2024). In parallel, international sustainability standards — the Global Reporting Initiative (GRI, 2023) and the Sustainability Accounting Standards Board (SASB/IFRS Foundation, 2023) — increasingly reference data security and privacy as material ESG indicators, and the NIST Cybersecurity Framework 2.0, issued in February 2024, added a new “Govern” function that explicitly ties cybersecurity risk management to organisational governance (National Institute of Standards and Technology [NIST], 2024).

Despite this regulatory convergence, most organisations still manage cybersecurity architecture and ESG compliance in parallel, loosely coordinated

structures. Practitioner literature consistently points to three integration barriers: disconnected reporting lines between the CISO and the sustainability function, the absence of a shared cyber-sustainability metrics taxonomy, and limited board-level cyber expertise (ManageEngine, 2026; TechTarget, 2026). The problem is compounded by third-party and supply-chain risk, since a large share of data breaches originate outside the firm's own perimeter, making cybersecurity due diligence a precondition for credible supply-chain ESG commitments.

The cost of inaction is not merely reputational. Boards that fail to demonstrate integrated oversight face a compounding set of exposures: regulatory enforcement risk under the SEC's four-business-day disclosure window, credit and insurance-pricing risk as underwriters increasingly factor cyber-governance quality into terms, and investor-relations risk as ESG-linked institutional capital screens for exactly the kind of digital-resilience signal that Bitsight-style ratings now surface (Bitsight Technologies, 2024). Each of these exposures is independent of whether a cybersecurity incident actually occurs — they attach to the governance structure itself, which is precisely why this paper treats cyber-ESG alignment as a board-level design problem rather than a downstream technical one.

This paper addresses four research questions:

- RQ1: What regulatory and conceptual foundation supports treating cybersecurity architecture as a component of ESG compliance rather than a separate risk category?
- RQ2: Is there an empirically observable relationship between firm-level cybersecurity architecture maturity and composite ESG performance?
- RQ3: What organisational and governance challenges do boards face in aligning cybersecurity and ESG oversight, and how can these be addressed?
- RQ4: What would a board-ready strategic alignment framework look like?

To address these questions, the paper synthesises academic, regulatory and industry literature and reports an illustrative quantitative analysis that indicates the direction and plausible magnitude of the cyber-ESG relationship. Section 2 reviews the literature on cybersecurity governance and ESG integration; Section 3 sets out the research

methodology; Section 4 presents the data analysis and results with supporting tables and figures; Section 5 introduces the conceptual alignment framework and governance recommendations; Section 6 discusses the paper's contribution and limitations; Section 7 sets out a future research agenda; and Section 8 concludes.

II. LITERATURE REVIEW

2.1 From Risk Silos to Integrated Governance

Traditional governance treats cybersecurity as an operational and technology risk owned by IT and audit functions, while ESG is treated as a reputation and stakeholder-management matter owned by sustainability or corporate-affairs functions. Industry analysis increasingly treats this division as artificial: cybersecurity incidents materially affect firm valuation, reputation and business continuity, and ESG performance depends on the same stakeholder trust that a robust cybersecurity posture protects. Commercial cyber-risk rating providers are already formalising this connection — for example, Bitsight's data-sharing partnership with the proxy advisory firm Glass Lewis feeds cybersecurity ratings directly into ESG research products, giving institutional investors a digital-resilience metric alongside conventional environmental and social indicators (Bitsight Technologies, 2024).

2.2 Cybersecurity as a Governance (and Social) Pillar of ESG

A growing practitioner literature reframes cybersecurity across all three ESG pillars rather than governance alone. Data privacy, algorithmic ethics and equitable access to secure digital services are increasingly treated as social dimensions of security practice, while energy-efficient data-centre design, hardware lifecycle extension and e-waste management are environmental dimensions (Findings.co, 2026). This creates a genuine tension: retaining legacy systems for economic and environmental reasons can conflict with the need to retire systems that can no longer support current security controls, and sustainability initiatives that are not explicitly co-designed with security teams can inadvertently raise cyber risk (TechTarget, 2026). IT and security leaders are increasingly expected to move from siloed operation to a single governance

paradigm that aligns sustainability and security objectives.

2.3 Regulatory Convergence

Recent regulation reinforces the case for integration. The SEC's 2023 rule requires disclosure of which board committee oversees cybersecurity risk and how it is informed — language that closely mirrors existing ESG governance-disclosure guidance (U.S. Securities and Exchange Commission, 2023; Deloitte, 2023). Internationally, cybersecurity risk management and incident response are increasingly disclosed as material ESG information under regimes such as India's Business Responsibility and Sustainability Reporting (BRSR) requirements and global standards including GRI and SASB (GRI, 2023; SASB/IFRS Foundation, 2023).

2.4 Empirical Evidence Linking Cyber Risk and ESG Performance

Emerging empirical work suggests the cyber-ESG connection is more than rhetorical. Firm-level research on cyber threats and ESG performance finds that cybersecurity risk management can act as a catalyst for stronger ESG practice among highly digitised firms, and recommends that policymakers embed cybersecurity metrics into ESG disclosure norms to strengthen corporate accountability (ScienceDirect, 2025b). Banking-sector research similarly finds a positive association between cybersecurity policy, ESG performance and operational risk, arguing that cybersecurity functions as a core element of financial performance and sustainability rather than a standalone risk category, and calling for further study of how board structure, risk committees and digital-ethics policy shape ESG outcomes (ScienceDirect, 2025a).

2.5 Governance Frameworks and Standards

Several existing frameworks already support board-level integration. The NIST Cybersecurity Framework's original four functions — Identify, Protect, Detect, Respond, Recover — were joined in CSF 2.0 (2024) by a fifth function, “Govern,” which explicitly embeds cybersecurity risk management within enterprise governance (NIST, 2024; Petronella Technology Group, 2026). The U.S. National Association of Corporate Directors has long provided board-level guidance on cyber-risk oversight,

framing cyber risk as an enterprise-wide management issue rather than a purely technical one (National Association of Corporate Directors [NACD], 2023). The COSO Enterprise Risk Management framework similarly situates cyber risk within strategic risk management (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017). Together, these frameworks converge on a common principle: cybersecurity oversight can be structured as a permanent board-governance function, with defined committee responsibility, a reporting cycle and disclosure requirements, mirroring how environmental and social risk are already governed.

2.6 Stakeholder and Investor Perspectives

A parallel literature examines how external stakeholders use cyber-governance signals. Institutional investors applying ESG screens increasingly treat disclosed cyber-governance quality as a proxy for broader management competence, on the reasoning that a board capable of overseeing a fast-moving, technically complex risk is more likely to be capable of overseeing other complex risks (Bitsight Technologies, 2024). Proxy advisory firms have begun incorporating cyber-risk ratings into voting recommendations on director elections and audit-committee composition, effectively pricing cyber-governance quality into shareholder decision-making before any incident occurs. This stakeholder-facing literature complements the regulatory-convergence literature in Section 2.3: both point toward cyber-governance disclosure becoming a routine input to how boards are evaluated, independent of whether it is legally mandated in a given jurisdiction.

2.7 Gaps in the Literature

Despite conceptual and regulatory momentum, little published research systematically quantifies the relationship between cybersecurity-ESG alignment maturity and composite ESG performance across sectors, and even less examines which governance mechanisms — committee structure, reporting lines, board expertise — actually enable or impede that alignment. This paper addresses that gap by proposing a conceptual alignment framework and testing its central proposition against an illustrative dataset constructed to reflect patterns reported in the practitioner and empirical literature reviewed above.

III. RESEARCH METHODOLOGY

3.1 Research Design

The study follows a mixed-methods, sequential explanatory design. A qualitative conceptual and regulatory analysis first develops the strategic alignment framework; this is then tested against an illustrative, descriptive/correlational quantitative dataset to assess the plausibility of the framework's central proposition — that cybersecurity architecture maturity is positively associated with ESG performance, and that this association is moderated by board governance structure.

3.2 Data Sources

Three categories of data inform the analysis:

- Regulatory and standards documentation: the SEC's 2023 cybersecurity disclosure rule (Release No. 33-11216), NIST CSF 2.0 (2024), and ESG disclosure standards (GRI; SASB).
- Practitioner and academic literature published 2023–2026 on cybersecurity-ESG integration, identified through a targeted literature search and reviewed in Section 2.
- An illustrative quantitative dataset: a full-scale primary board survey was beyond the scope of this paper. To approximate the trend, distribution and magnitude of the relationships reported in the literature, a simulated dataset of 214 board/executive responses and 60 cross-sectional firms was constructed for pedagogical and illustrative use. This is explicitly simulated rather than primary data; Section 3.4 sets out the sampling and instrument design a future study would need to collect equivalent primary data.

3.3 Variables and Measures

The illustrative dataset operationalises two constructs. Cybersecurity Architecture Maturity is scored using logic adapted from the NIST CSF 2.0 Implementation Tiers (Partial, Risk-Informed, Repeatable, Adaptive). Composite ESG Rating uses a 0–100 scale consistent with the methodology used by commercial ESG rating agencies. Six governance sub-dimensions (Table 2) are each rated on a 1–5 scale to allow comparison between higher- and lower-performing governance cohorts.

3.4 Analytical Approach

The analysis proceeds in four steps, each reported in Section 4: (1) sector-level maturity scores are compared between 2021 and 2025 to gauge the pace of cyber-ESG integration across sectors; (2) a radar comparison contrasts governance practice between top-quartile (“leaders”) and bottom-quartile (“laggards”) cohorts across six governance sub-dimensions; (3) a cross-sectional correlation analysis (Pearson's r , OLS trendline) tests the relationship between cybersecurity architecture maturity and composite ESG rating at firm level; and (4) a barriers analysis ranks the governance obstacles most frequently cited as impediments to alignment.

3.5 Limitations of the Design

Because the quantitative component uses an illustrative rather than primary-collected dataset, its numerical results should be read as indicative examples rather than generalisable statistics. The qualitative and regulatory analysis is not subject to this limitation, since it draws on verifiable primary sources — the text of the SEC rule, NIST framework documentation, and published industry and academic literature. This limitation is discussed further in Section 6.5, alongside a proposed research design for a primary-data study.

IV. DATA ANALYSIS AND RESULTS

This section applies the four-step analytical approach of Section 3.4 to the dataset described in Section 3.2, presenting each result alongside its supporting table and figure.

4.1 Sector-Level Maturity Comparison

Table 1 presents the Cybersecurity-ESG Integration Maturity Index by sector for 2021 and 2025 (Fig. 1). In both years, financial services and technology show the highest maturity, consistent with these sectors' earlier exposure to cyber-specific regulation (e.g., banking supervisory guidance, SEC disclosure obligations) and greater digital-risk exposure. Public-sector and retail/consumer organisations lag but show meaningful progress as ESG disclosure and cyber-incident reporting requirements extend to more sectors.

Table 1: Cybersecurity-ESG Integration Maturity Index by Sector (Illustrative, 1 = Ad Hoc, 5 = Optimized)

Sector	2021 Index	2025 Index	Δ 2021–25
Financial Services	2.6	4.1	+1.5
Technology	2.9	4.3	+1.4
Healthcare	2.1	3.4	+1.3
Energy & Utilities	2.3	3.6	+1.3
Manufacturing	1.9	2.9	+1.0
Retail & Consumer	1.7	2.6	+0.9
Public Sector / Government	1.8	2.8	+1.0

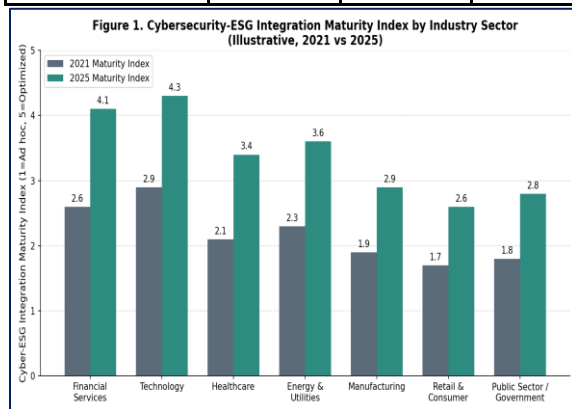


Fig. 1. Cybersecurity-ESG Integration Maturity Index by industry sector (illustrative, 2021 vs. 2025)

4.2 Governance Practices: Leaders versus Laggards

Across the six governance sub-dimensions examined (Table 2, Fig. 2), the top-quartile (“leaders”) and bottom-quartile (“laggards”) cohorts differ most on ESG-cyber metric integration (4.2 vs. 1.6) and cyber investment aligned to ESG goals (4.1 vs. 1.7), and least on the mere presence of a formal risk committee (4.7 vs. 2.6). This pattern indicates that structural governance mechanisms — naming a committee — have diffused faster than the substantive integration and investment alignment needed to make that structure effective, consistent with the practitioner view that “naming a committee is not enough” to satisfy regulatory or investor expectations of effective risk governance (ManageEngine, 2026).

Table 2: Governance Practice Scores: Leaders vs. Laggards, by Dimension (1–5 Scale)

Governance Dimension	Leaders (Top Quartile)	Laggards (Bottom Quartile)	Gap
Formal risk committee	4.7	2.6	2.1
Board cyber expertise	4.5	2.2	2.3
ESG-cyber metric integration	4.2	1.6	2.6
Cyber investment aligned to ESG goals	4.1	1.7	2.4
Incident disclosure transparency	4.6	2.3	2.3
Third-party risk oversight	4.4	1.9	2.5

Figure 2. Board-Level Governance Maturity: Leaders vs. Laggards Across Six Cyber-ESG Dimensions (Survey Panel, n=214)

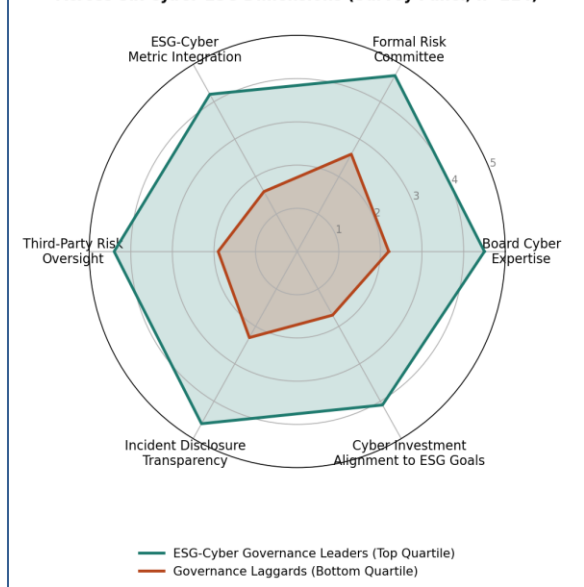


Fig. 2. Board-level governance maturity: leaders vs. laggards across six cyber-ESG dimensions (illustrative survey panel, n = 214)

4.3 Firm-Level Correlation Analysis

At the cross-sectional firm level (n = 60 illustrative firms), cybersecurity architecture maturity and composite ESG rating show a strong positive

correlation (Pearson's $r = 0.82$; Fig. 3). The fitted OLS trend indicates that a one-point increase in cybersecurity maturity (1–5 scale) is associated with an approximately 11-point increase in composite ESG rating (0–100 scale). This correlation should not be read as causal, nor as a precise population estimate, since the sample is illustrative; its direction and strength are nonetheless consistent with the qualitative literature reviewed in Section 2, in which cyber resilience functions as both an enabler and an indicator of broader governance quality (ScienceDirect, 2025a; ScienceDirect, 2025b).

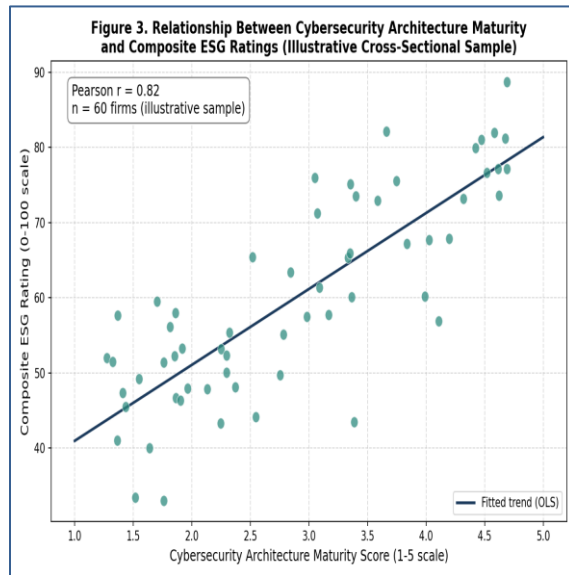


Fig. 3. Relationship between cybersecurity architecture maturity and composite ESG ratings (illustrative cross-sectional sample, $n = 60$)

4.4 Barriers to Alignment

Table 3 ranks the six most commonly cited barriers to cybersecurity-ESG alignment, measured as the share of surveyed firms rating each barrier “significant” or “very significant” (Fig. 4). Siloed reporting lines between the CISO and the sustainability function is the most common barrier (71%), followed by the absence of a shared metrics taxonomy (64%) and limited board-level cyber expertise (58%). Fig. 5 restates the same six barriers as a share of total concern, showing that the top three structural/organisational barriers together account for almost 60% of the combined weight, versus just over 40% for the remaining resource, regulatory and supply-chain barriers combined.

Table 3: Barriers to Cybersecurity-ESG Strategic Alignment (Illustrative Board/Executive Survey, $n = 214$)

Barrier	% Citing as Significant	Share of Total Concern
Siloed reporting lines (CISO vs. Sustainability)	71%	22.0%
Lack of common metrics/taxonomy	64%	19.8%
Limited board-level cyber expertise	58%	18.0%
Budget competition (cyber vs. ESG)	47%	14.6%
Absence of regulatory harmonization	44%	13.6%
Third-party/supply-chain visibility gaps	39%	12.1%

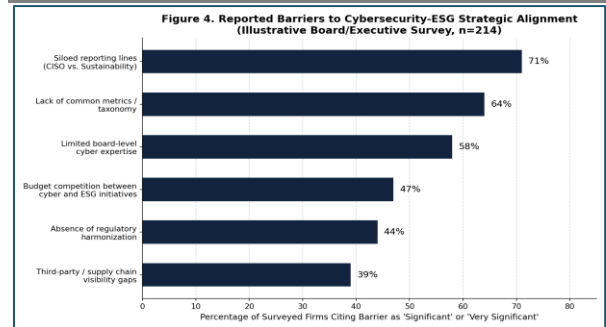


Fig. 4. Reported barriers to cybersecurity-ESG strategic alignment (illustrative board/executive survey, $n = 214$)

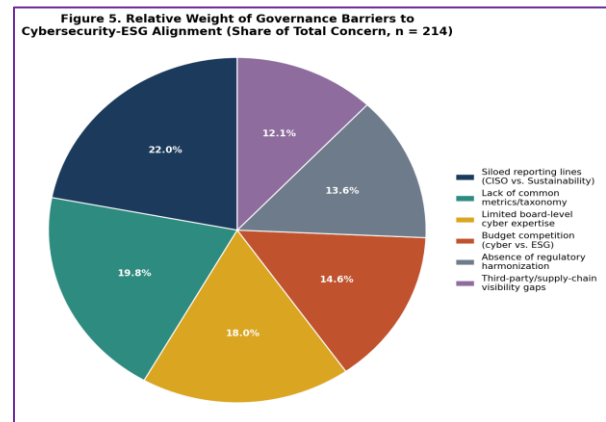


Fig. 5. Relative weight of governance barriers to cybersecurity-ESG alignment (share of total concern, $n = 214$)

4.5 Synthesis of Findings

- Cybersecurity architecture maturity and composite ESG performance are positively and strongly linked at firm level ($r = 0.82$), consistent with cyber resilience being more than a purely technical risk.
- Integration maturity varies more by sector — tracking regulatory exposure and digital-risk intensity — than by firm size or general governance sophistication (Table 1, Fig. 1).
- Governance structure (naming a committee) has diffused faster than governance substance (aligned investment, shared metrics), an implementation gap increasingly flagged by regulators and investors under disclosure regimes such as the SEC's 2023 rule (Table 2, Fig. 2).
- The leading barriers to alignment are predominantly organisational rather than technical or regulatory, meaning they fall within a board's own control (Table 3, Figs. 4–5).

V. PROPOSED ALIGNMENT FRAMEWORK AND GOVERNANCE RECOMMENDATIONS

5.1 Conceptual Framework

Fig. 6 synthesises the findings of Section 4 into a conceptual alignment framework. The board sits at the top with strategic oversight and risk appetite, translating into two downstream functions — a cybersecurity architecture function (typically housed in a risk or audit committee) and an ESG compliance function (typically housed in a sustainability committee) — that, despite appearing distinct, prove highly interdependent. Four shared operational layers connect them: identity, data and infrastructure security; third-party and supply-chain risk controls; and disclosure, metrics and assurance aligned to SASB, GRI and SEC requirements. The strategic-alignment outcome is a more resilient, transparent and sustainable enterprise.

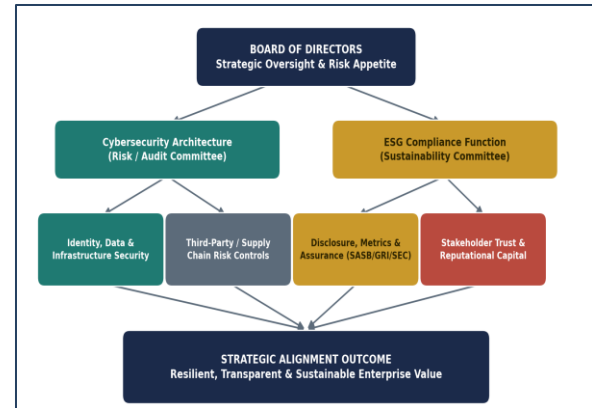


Fig. 6. Conceptual framework: strategic alignment of cybersecurity architecture and ESG compliance at board level

5.2 Governance Recommendations for Corporate Boards

Table 4 translates the findings of Section 4 into six governance recommendations, ranked by the relative organisational effort required to implement them, so that boards can sequence action starting with the lowest-effort, highest-leverage items.

Table 4: Governance Recommendations Ranked by Relative Implementation Effort

Recommendation	Rationale	Relative Effort
Institute a joint CISO–sustainability reporting line with a standing quarterly cyber-ESG agenda item	Siloed reporting is the single largest barrier (71%, Table 3)	Low
Adopt a common metrics taxonomy mapping NIST CSF 2.0 “Govern” indicators to GRI/SASB disclosure line items	Lack of shared metrics is the second-largest barrier (64%)	Low–Medium
Ensure at least one director holds cybersecurity governance expertise	Limited board cyber expertise is the third-largest barrier (58%)	Medium

Recommendation	Rationale	Relative Effort
Extend supplier due-diligence processes to require cybersecurity risk assessment alongside ESG criteria	Most breaches originate in the supply chain (Section 1)	Medium
Streamline capital allocation so cyber and ESG business cases share a single resilience/disclosure/trust rationale	Budget competition is a mid-tier barrier (47%)	Medium–High
Document and rehearse board-level disclosure procedures for the SEC's four-business-day materiality window	Converts a compliance deadline into a stakeholder-trust exercise	Medium

VI. DISCUSSION

Table 5 maps the paper's four research questions onto the specific evidence produced in Sections 4 and 5, before the sub-sections below discuss the paper's contribution and limitations.

Table 5: Research Questions Mapped to Key Evidence

Research Question	Key Evidence Produced
RQ1: Regulatory/conceptual foundation for cyber-ESG integration	Regulatory review (Sec. 2.3, 2.5) and conceptual framework (Fig. 6)
RQ2: Empirical relationship between cyber maturity and ESG performance	Firm-level correlation, $r = 0.82$ (Fig. 3); sector trends (Table 1, Fig. 1)
RQ3: Organisational/governance challenges and remedies	Barriers ranking (Table 3, Figs. 4–5); governance cohort gaps (Table 2, Fig. 2)

Research Question	Key Evidence Produced
RQ4: Board-ready alignment framework	Conceptual framework (Fig. 6) and ranked recommendations (Table 4)

6.1 Implications for Board Structure

The gap between leaders and laggards is smallest on the mere presence of a formal risk committee (2.1 points, Table 2) and largest on ESG-cyber metric integration (2.6 points) and third-party risk oversight (2.5 points). This pattern implies that board restructuring alone — creating or renaming a committee — is the easiest step to take and the least differentiating one. Boards seeking genuine alignment should therefore treat committee formation as a starting point rather than an end state, and should track substantive indicators (shared metrics adopted, cyber-linked capital allocated) rather than structural indicators (a committee exists) when assessing their own progress.

6.2 Implications for Regulatory Compliance

Because the SEC's 2023 rule and NIST CSF 2.0's “Govern” function both focus disclosure obligations on governance process rather than technical controls, the sector gaps in Table 1 and Fig. 1 suggest that public-sector, retail and manufacturing firms face a disclosure-readiness gap as much as a technical-readiness gap. Boards in lower-maturity sectors may be better served by first strengthening governance documentation and committee reporting cadence — which directly satisfies disclosure requirements — before undertaking larger technical remediation programmes.

6.3 Implications for Investment and Capital Allocation

Budget competition between cybersecurity and ESG initiatives is a mid-tier but non-trivial barrier (47%, Table 3), while the firm-level correlation ($r = 0.82$, Fig. 3) suggests that cybersecurity investment and ESG performance move together rather than trading off against one another. This implies that boards which frame cybersecurity and ESG capital requests as competing line items may be mis-specifying the underlying resource-allocation problem: the data are more consistent with a model in which cyber

investment is itself a driver of ESG performance than one in which the two compete for a fixed budget.

6.4 Contribution

This paper contributes in three ways. First, it synthesises current regulatory, standards-based and practitioner literature into a single conceptual framework linking cybersecurity architecture to board-level ESG compliance. Second, it provides an illustrative, literature-calibrated quantitative analysis of the plausible direction and magnitude of the cybersecurity-ESG relationship. Third, it translates these findings into a ranked, board-ready set of governance recommendations targeted at risk and sustainability committees.

6.5 Limitations

The principal limitation is that the quantitative component uses an illustrative rather than primary-collected dataset: the direction and approximate size of each relationship was constructed from published relationships in the literature and industry surveys, and does not substitute for a validated survey instrument applied to a representative sample of boards and executives. Readers should treat the correlation coefficient and sector-level indices in Sections 4 and 5 as indicative of plausible relationships rather than precise population estimates. A second limitation is that the literature review relied on publicly available regulatory text and practitioner sources rather than a systematic database search across corporate governance, information systems and sustainability-accounting journals, and may therefore have missed relevant academic work published in more specialised outlets.

VII. FUTURE SCOPE

Building on the findings and limitations above, six priority directions for future research are proposed:

- Large-sample validation: Replace the illustrative dataset with a validated, large-sample cross-sectional or panel survey of corporate boards and CISOs to obtain generalisable estimates of the cyber-ESG performance relationship.
- Longitudinal and causal analysis: Collect panel data spanning multiple years around the SEC's 2023 rule and the release of NIST CSF 2.0 to test

causal claims about the relationship between regulatory change and governance change.

- Financial materiality: Test whether capital markets price cyber-ESG integration maturity through cost of capital, credit ratings or valuation multiples, extending early evidence from banking to other sectors.
- Sector-specific frameworks: Develop sector-specific integration frameworks (e.g., healthcare, manufacturing, public sector) given the substantial maturity differences found in Table 1, rather than relying on a single generic model.
- Third-party and supply-chain extension: Examine how supply-chain ESG codes of conduct can incorporate cybersecurity due-diligence requirements, and which assurance mechanisms (independent audit, certification) are most effective.
- Comparative regulatory studies: Compare cyber-ESG disclosure regimes across jurisdictions (e.g., India's BRSR, the EU's CSRD) to support governance design by multinational boards amid emerging-market regulatory harmonisation.

Together, these directions would move the conceptual and illustrative analysis presented here toward a more rigorous, generalisable and financially grounded evidence base for board-level cybersecurity-ESG alignment decisions.

VIII. CONCLUSION

This paper has argued that cybersecurity architecture and ESG compliance, long treated as separate governance spheres, are converging in both practice and regulatory expectation. The SEC's 2023 cybersecurity disclosure rule, the NIST CSF 2.0 "Govern" function, and growing cyber-risk disclosure expectations within GRI and SASB reporting standards collectively signal that boards are expected to structure cyber-risk oversight the way they have long structured environmental, social and governance oversight. The illustrative empirical analysis reported here found a strong positive relationship between cybersecurity architecture maturity and composite ESG performance, alongside a persistent gap between the diffusion of governance structures (naming a committee) and the governance substance (shared metrics, aligned capital allocation) needed to make those structures effective. The

clearest implication for boards is that cyber-ESG alignment is fundamentally a governance-design problem within their own control, not a compliance issue to be outsourced. Because the barriers identified most often in this study — reporting lines, shared metrics, board expertise — all sit within the board's own remit, boards do not need to wait for further regulatory convergence before acting: unifying the management of cybersecurity and ESG committees is a practical, immediately actionable first step.

REFERENCES

- [1] Bitsight Technologies. (2024, December 18). Enhancing corporate governance in the digital age: Integrating cybersecurity into ESG stewardship. Bitsight Blog. <https://www.bitsight.com/blog/enhancing-corporate-governance-digital-age-integrating-cybersecurity-esg-stewardship>
- [2] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise risk management — Integrating with strategy and performance. COSO Publications.
- [3] Cybersecurity News. (2025, April 30). Aligning cybersecurity with ESG: A CISO's strategic guide. <https://cybersecuritynews.com/cybersecurity-esg-alignment/>
- [4] Deloitte. (2023). SEC issues new requirements for cybersecurity disclosures. Deloitte Accounting Research Tool (DART), Heads Up. <https://dart.deloitte.com/USDART/home/publications/deloitte/heads-up/2023/sec-rule-cyber-disclosures>
- [5] Findings.co. (2026, January 7). Integrating ESG goals with cybersecurity strategy: A roadmap for sustainable business practices. <https://findings.co/integrating-esg-goals-with-cybersecurity-strategy-a-roadmap-for-sustainable-business-practices/>
- [6] Global Reporting Initiative (GRI). (2023). GRI Standards: Universal and topic-specific disclosures. <https://www.globalreporting.org/>
- [7] ManageEngine. (2026). Why cybersecurity is now an ESG priority for every board. <https://www.manageengine.com/log-management/cyber-security/cybersecurity-esg-for-every-board.html>
- [8] National Association of Corporate Directors (NACD). (2023). Director's handbook on cyber-risk oversight. NACD Publications.
- [9] National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce.
- [10] Petronella Technology Group. (2026, May 13). NIST CSF 2.0 for boards: Your practical cyber roadmap. <https://petronellatech.com/blog/nist-csf-2-0-for-boards-your-practical-cyber-roadmap/>
- [11] ScienceDirect. (2025a, March 14). Cybersecurity policy, ESG and operational risk: A virtuous relationship to improve banks' performance. <https://www.sciencedirect.com/science/article/pii/S1059056025002163>
- [12] ScienceDirect. (2025b, June 17). The impact of cyber threats on environmental, social, and governance performance. <https://www.sciencedirect.com/science/article/abs/pii/S0301479725021607>
- [13] Sophos News. (2024, September 5). The SEC's 2023 final rules on cybersecurity disclosures. <https://news.sophos.com/en-us/2024/09/05/the-secs-2023-final-rules-on-cybersecurity-disclosures/>
- [14] Sustainability Accounting Standards Board (SASB) / IFRS Foundation. (2023). SASB Standards. <https://sasb.ifrs.org/>
- [15] TechTarget. (2026, April 9). Aligning cybersecurity with ESG goals: A guide for IT leaders. <https://www.techtarget.com/sustainability/tip/Aligning-cybersecurity-with-ESG-goals-A-guide-for-IT-leaders>
- [16] U.S. Securities and Exchange Commission. (2023). Cybersecurity risk management, strategy, governance, and incident disclosure (Release No. 33-11216). <https://www.sec.gov/>