INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XII, December 2025

Strategic Leadership and Cybersecurity Readiness in Digitally Transforming Organisations

Destiny Young [1, *], Osinachi Ozocheta[2]

[1] Oil and Gas Free Zones Authority Onne, Rivers State, Nigeria

[2] Stowe School Buckingham, United Kingdom

DOI : https://doi.org/10.51583/IJLTEMAS.2025.1412000004

Received: 10 December 2025; Accepted: 17 December 2025; Published: 25 December 2025

ABSTRACT

Cybersecurity readiness has become a material organisational capability as digital transformation expands attack surfaces and regulatory scrutiny. Existing research and practice guidance largely frame readiness as a function of technical controls and compliance maturity, offering limited explanation of how executive leadership structures shape sustained resilience. This paper advances a theory building perspective that conceptualises cybersecurity readiness as an outcome of strategic leadership rather than a purely technical condition.

Drawing on strategic leadership theory, enterprise risk management, and cyber risk quantification literature, the study develops a Strategic Cyber Leadership Model that integrates four core elements: distributed C suite accountability as a leadership input, Cyber Risk Quantification as a financial decision-making mechanism, enterprise-wide risk integration as a governance amplifier, and measurable readiness outcomes. The model explicitly incorporates contextual moderators, including regulatory intensity and digital transformation level, to explain variation in readiness across organisations and sectors.

Five research propositions are advanced to articulate the causal relationships within the model, positioning the paper as a foundation for future empirical testing. By shifting the analytical focus from control inventories to leadership driven governance mechanisms, this study contributes to cybersecurity and management scholarship while offering a coherent conceptual framework for boards and senior executives seeking to institutionalise cyber resilience as a strategic capability.

Keywords: Strategic leadership, Cybersecurity readiness, Cyber Risk Quantification, Enterprise Risk Management, Digital transformation, Governance

INTRODUCTION

The modern organisation operates within a digital ecosystem characterised by continuously expanding attack surfaces, increasingly sophisticated adversarial tactics, and heightened regulatory demands (DNV, n.d.). Digitalisation provides opportunities for innovation and market growth but simultaneously introduces profound strategic vulnerabilities (CISA, n.d. c; StrongBox IT, 2025). Consequently, failure in cybersecurity is widely acknowledged as a major global threat, capable of inflicting severe financial, operational, and reputational damage upon the modern enterprise (StrongBox IT, 2025; Principles for Board Governance of Cyber Risk, 2021).

Organisational resilience is no longer an optional technical measure but a fundamental requirement for success, requiring robust capabilities to identify, prevent, and effectively respond to cyber threats (BitSight Technologies, 2023). Despite this imperative, a high percentage of

security leaders express low confidence in their company's overall security posture, indicating a pervasive struggle to achieve adequate readiness (BitSight Technologies, 2023). This persistent performance gap underscores the essential need for strong **strategic leadership**, defined as the executive capacity required to

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XII, December 2025

align cybersecurity strategy with business objectives, secure necessary resources, and rigorously enforce accountability across the enterprise (StrongBox IT, 2025).

This paper develops a cohesive conceptualisation of effective strategic leadership necessary for sustainable cybersecurity readiness in digitally transforming organisations. Section 2 establishes the conceptual background relating to governance and the required distribution of accountability across the C suite, highlighting the current gaps in practice. Section 3 details the conceptual methodology, focusing on the synthesis of risk management concepts and frameworks. Section 4 presents the analysis of core mechanisms for readiness, including executive accountability, risk quantification, and performance measurement. Section 5 provides discussion points on operational readiness and systemic risk mitigation using rigorous frameworks. Finally, Section 6 offers conclusions and actionable recommendations for building sustained resilience against contemporary challenges.

RELATED LITERATURE

The Mandate for Strategic Governance and Fiduciary Duty

Cyber risk has transitioned unequivocally from a technical problem confined to the Information Technology department to a material business risk requiring formalized oversight at the highest executive levels (Aon, 2025; StrongBox IT, 2025). This strategic elevation is necessary because cyber incidents have repeatedly demonstrated the capacity to inflict severe financial and operational impacts on an organisation's market valuation and long term stability (FS-ISAC, 2021). Boards of directors are ethically and legally obligated to understand the organisation's cyber posture and the prevailing threat landscape to properly execute their fiduciary duties to shareholders (FS-ISAC, 2021; Principles for Board Governance of Cyber Risk, 2021).

Effective governance, therefore, requires a comprehensive strategy that integrates with overall organisational operations, aiming to prevent the interruption of activities due to cyberattacks (CISA Governance, n.d.). Features of successful cybersecurity governance include: formal accountability frameworks, defined decision-making hierarchies, established risks explicitly linked to business objectives, mitigation plans, and robust oversight processes (CISA Governance, n.d.). Crucially, boards must set the organisation's risk tolerance or risk appetite, guiding management in setting security strategy and investment decisions (Principles for Board Governance of Cyber Risk, 2021; FS-ISAC, 2021). The elevation of cyber risk mandates that executive leaders take urgent, high impact actions to enhance corporate resilience in today's complex technical environment (CISA, n.d. c).

Strategic Leadership and Distributed Executive Accountability

Cybersecurity effectiveness fundamentally relies on the clear definition and execution of accountability across the entire senior leadership team (StrongBox IT, 2025). This requires the responsibility to be intentionally broadened beyond the Chief Information Security Officer and Chief Information Officer to encompass the full C suite, reflecting its status as an enterprise-wide concern (StrongBox IT, 2025).

The Chief Executive Officer is the ultimate champion, setting the strategic vision and ensuring a security focused culture is developed throughout the workplace (StrongBox IT, 2025; CISA, n.d. c). The CEO also approves budgets for security initiatives and maintains accountability for the organisation's security posture (StrongBox IT, 2025). The Chief Financial Officer holds primary responsibility for financial risk management, including budgeting for tools, managing regulatory compliance costs, and assessing the financial impact of potential threats (StrongBox IT, 2025).

The Chief Operating Officer is tasked with ensuring that cybersecurity practices are integrated directly into operational business processes, managing operational risk, overseeing supply chain security, and coordinating cross functional incident response (StrongBox IT, 2025). The Chief Human Resources Officer manages the human risk vector, implementing compulsory employee training, mitigating insider threats, and securing employee data privacy (StrongBox IT, 2025). Since the vast majority of cyberattacks involve a human element, the CHRO's role is critical in fostering a security aware workforce (StrongBox IT, 2025; BitSight Technologies, 2023). This unified leadership cooperation represents the foundational defense mechanism against contemporary cyber threats (StrongBox IT, 2025).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XII, December 2025

Integrating Cyber Risk into Enterprise Risk Management (ERM)

To ensure consistent and holistic management, cyber risk must be fully integrated into the broader Enterprise Risk Management (ERM) framework (Aon, 2025). This integration ensures that cyber risks are assessed alongside other intersectional enterprise risks, such as business interruption or supply chain failures (Aon, 2025). This alignment amplifies the effectiveness of both disciplines by improving information sharing, strengthening cyber practices, and enabling more efficient resource deployment (Aon, 2025).

Cyber risk management and ERM share foundational components, including structured Risk Identification and Assessment, formalized Risk Response Planning, robust Monitoring and Reporting mechanisms, and defined Governance and Oversight structures (Aon, 2025). Successful integration mandates that security leaders establish organizational standards that align with widely accepted cyber security frameworks, such as the NIST Cybersecurity Framework or ISO 27001 (Aon, 2025; Complyance, 2025). These frameworks provide the basis for establishing control baselines, identifying areas for improvement, and accurately tracking progress towards defined standards (Aon, 2025).

Cyber Risk Quantification (CRQ) and Value Translation

A critical strategic necessity for modern cybersecurity leaders is the ability to translate complex technical risks into financial terms that resonate with executive leadership, a process known as Cyber Risk Quantification (Balbix, 2025; SecurityScorecard, 2025a; SecurityScorecard, 2025c). CRQ

assesses and calculates the potential financial impact of cyber threats, transforming conversations from technical jargon into monetary risk exposure (Balbix, 2025; SecurityScorecard, 2025a).

This quantitative approach helps organisations understand the monetary value of their risk exposure, which enables informed decision-making regarding resource allocation (Balbix, 2025). By quantifying risks in currency terms, security leaders can objectively prioritise security investments based on which actions deliver the greatest reduction in financial risk

(SecurityScorecard, 2025a; Balbix, 2025). This approach helps security teams to justify spending, moving cybersecurity beyond the perception of a cost center to an investment that drives business resilience and supports growth (Complyance, 2025; Balbix, 2025). The ability to articulate cyber risk in business terms also fosters crucial collaboration among security professionals, business leaders, and stakeholders (SecurityScorecard, 2025c).

Gaps Identified in Current Practices

Despite the clear mandates for strategic leadership, several pervasive gaps hinder the transition to enterprise-wide cybersecurity readiness. A significant strategic challenge is the communication and alignment gap; different organisational functions often **do not speak the same language** regarding cybersecurity, which impedes the ability to **gain necessary buy in for investments** and ensures a lack of **sufficient focus during the planning stages** of projects (DNV, n.d.). Security leaders frequently struggle to **translate complex technical risks into business language** that clearly articulates the business implications for executive leadership (Complyance, 2025; SecurityScorecard, 2025b).

This communication failure contributes directly to financial and operational misalignment. For example, research indicates that **only half of executives significantly measure the financial impact of cyber risks**, resulting in **misallocated resources** and leaving the organisation poorly prepared for threats (PwC, 2026; SecurityScorecard, 2025b; SecurityScorecard, 2025a). Operationally, organisations continue to rely heavily on **traditional risk assessments that capture only a point in time snapshot** of the security posture, failing to keep pace with the rapidly changing and highly dynamic digital ecosystem (SecurityScorecard, 2025c; BitSight Technologies, 2023). Strategic leadership is also challenged because cybersecurity strategies often **do not consider specific organisational factors** such as existing culture, level of maturity, or regulatory differences, which prevents tailored and efficient security implementations (DNV, n.d.). These shortfalls highlight the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XII, December 2025

continuing necessity for strategic leaders to move beyond compliance checklists towards integrated, quantitative, and culturally embedded risk management practices (PwC, 2026; Principles for Board Governance of Cyber Risk, 2021).

METHODOLOGY

This paper adopts a structured conceptual synthesis methodology aimed at theory development rather than empirical generalisation. Source identification was conducted through targeted searches of Scopus, Web of Science, and Google Scholar, alongside official repositories of regulatory and standards bodies. The review covered materials published between 2019 and 2025 to reflect contemporary digital transformation and regulatory conditions.

Included sources comprised peer reviewed academic articles, international standards, regulatory guidance, and high credibility practitioner reports that explicitly addressed cybersecurity governance, executive leadership, cyber risk quantification, or enterprise risk management. Practitioner and vendor publications were included only where they contributed conceptual insight into emerging risk quantification or automation mechanisms and were triangulated against academic or regulatory sources.

Conceptual convergence across independent sources was prioritised during synthesis. Where conflicting recommendations emerged, preference was given to those aligned with internationally recognised standards or supported by multiple independent bodies. The outcome of this process is an integrated conceptual model that explains how strategic leadership mechanisms shape cybersecurity readiness.

Strategic Cyber Leadership Model

This study advances cybersecurity scholarship by theorising readiness as a strategic leadership outcome rather than a purely technical or compliance driven condition. Existing frameworks, including NIST CSF 2.0 and the CISA Cybersecurity Performance Goals, articulate recommended practices but do not explicate the organisational mechanisms through which executive leadership converts governance intent into sustained cyber readiness.

Figure 1: The Strategic Cyber Leadership Model

The figure above presents the Strategic Cyber Leadership Model, which theorises cybersecurity readiness as a leadership driven outcome. The model illustrates how distributed C suite accountability operates as the primary

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XII, December 2025

input, influencing readiness through the mediating mechanism of Cyber Risk Quantification and the amplifying effect of Enterprise Risk Management integration. Readiness outcomes are expressed through measurable indicators such as detection speed, response effectiveness, and incident impact. Contextual moderators, including digital transformation intensity, sectoral regulation, and jurisdictional requirements, condition the strength of these relationships. The model extends existing cybersecurity frameworks by explicitly articulating the causal pathways through which executive leadership structures translate governance intent into operational resilience.

The Strategic Cyber Leadership Model integrates four analytically distinct components into a single causal structure. Executive accountability across the C suite constitutes the primary leadership input. Cyber Risk Quantification functions as the financial decision-making mechanism that translates technical exposure into business relevant risk signals. Enterprise Risk Management integration operates as a governance amplifier that aligns cyber risk with broader organisational risk priorities. Cyber readiness metrics represent the observable outcomes of this leadership process.

Contextual factors, including the organisation's level of digital transformation, sectoral regulation, and jurisdictional requirements, moderate the strength of these relationships. The model therefore extends existing guidance by explaining how leadership structures and financial logic determine whether frameworks translate into operational resilience.

Research Propositions

The Strategic Cyber Leadership Model gives rise to the following propositions, which are intended to guide future empirical research.

P1: Higher levels of distributed C suite cybersecurity accountability are positively associated with organisational cybersecurity readiness.

P2: Cyber Risk Quantification mediates the relationship between executive accountability and effective cybersecurity investment decisions.

P3: Integration of cyber risk into Enterprise Risk Management strengthens the relationship between Cyber Risk Quantification and cybersecurity readiness outcomes.

P4: Regulatory intensity positively moderates the relationship between governance maturity and cybersecurity readiness.

P5: The level of digital transformation positively moderates the effect of strategic leadership on cybersecurity readiness.

Data Analysis and Presentation

The analysis of the required components of strategic cybersecurity leadership yields three primary models illustrating accountability, risk financialisation, and mandated operational structure. These models collectively demonstrate how strategic leaders translate the governance mandate into measurable readiness outcomes.

Executive Accountability and Cross Functional Responsibility

Effective strategic governance requires definitive roles and responsibilities to be established and enforced across the senior leadership team (StrongBox IT, 2025). This analysis, summarised below in Table 1, highlights the critical shift from a siloed technical ownership to a distributed enterprise risk mandate, vital for building a unified security culture (StrongBox IT, 2025; CISA, n.d. c).

The table below enhances clarity by defining how each executive contributes uniquely to overall cyber readiness and resilience beyond the traditional CISO function.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XII, December 2025

Executive Accountability Inputs within the Strategic Cyber Leadership Model

Leadership Role	Strategic Accountability Input	Governance Lever	Contribution to Readiness Outcome
Board of Directors	Define cyber risk appetite and oversight expectations	Fiduciary oversight, performance monitoring	Aligns cybersecurity priorities with enterprise value protection and regulatory compliance
Chief Executive Officer	Enterprise-wide accountability for cyber risk	Strategic mandate, resource authorisation	Embeds cybersecurity into organisational strategy and culture
Chief Financial Officer	Financial interpretation of cyber risk	Budget governance, capital allocation	Enables risk informed investment decisions through CRQ
Chief Operating Officer	Operational integration of security controls	Process ownership, business continuity governance	Ensures resilience of core operations and supply chains
Chief Human Resources Officer	Management of human cyber risk	Workforce policy, training governance	Reduces insider risk and strengthens security culture
Chief Information Security Officer	Translation of technical risk into business terms	Risk assessment, control strategy	Operationalises leadership intent into measurable readiness

Table 1: Executive Accountability Inputs within the Strategic Cyber Leadership Model

Table 1 positions executive roles as leadership inputs within the Strategic Cyber Leadership Model rather than as isolated functional responsibilities. Each role contributes a distinct governance lever that collectively shapes the organisation's ability to convert strategic intent into sustained cybersecurity readiness.

The Cyber Risk Financialisation Framework

Cyber Risk Quantification (CRQ) provides the strategic link between governance decisions (Table 1) and resource allocation, helping executives understand the monetary value of risks (Balbix, 2025; SecurityScorecard, 2025a). CRQ facilitates investment justification by focusing on the reduction of financial risk exposure, ensuring that security spending delivers measurable Return on Security Investment (SecurityScorecard, 2025a; Balbix, 2025). Figure 1 conceptually illustrates this systematic process, which should serve as the blueprint for resource governance.

Cyber Risk Quantification links executive governance decisions to measurable investment outcomes by translating technical exposure into financial risk estimates.

Despite its strategic value, Cyber Risk Quantification is subject to important limitations. Quantitative models depend on assumptions regarding threat frequency, loss magnitude, and control effectiveness, which may be unstable for low frequency, high impact cyber events. Over reliance on numeric outputs can generate false precision and obscure qualitative risk signals. Strategic leadership must therefore position CRQ as a decision support mechanism that complements scenario analysis and expert judgement rather than a deterministic predictor of loss.

Foundational Frameworks for Operational Structure

Organisational readiness must be anchored in internationally recognised, adaptable security frameworks. The NIST Cybersecurity Framework (CSF) 2.0 provides the essential strategic blueprint for managing cyber risks

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XII, December 2025

across all organizational sizes and sectors (NIST, 2024). The CSF Core organises cybersecurity outcomes into six integrated Functions, establishing a common lexicon for practitioners and executives (NIST, 2024). Figure 2 visually represents this structure, which serves as the strategic taxonomy for organizing operational activities.

This visual aid clarifies the hierarchical nature of the Functions, emphasising that **GOVERN** is central to all other activities.

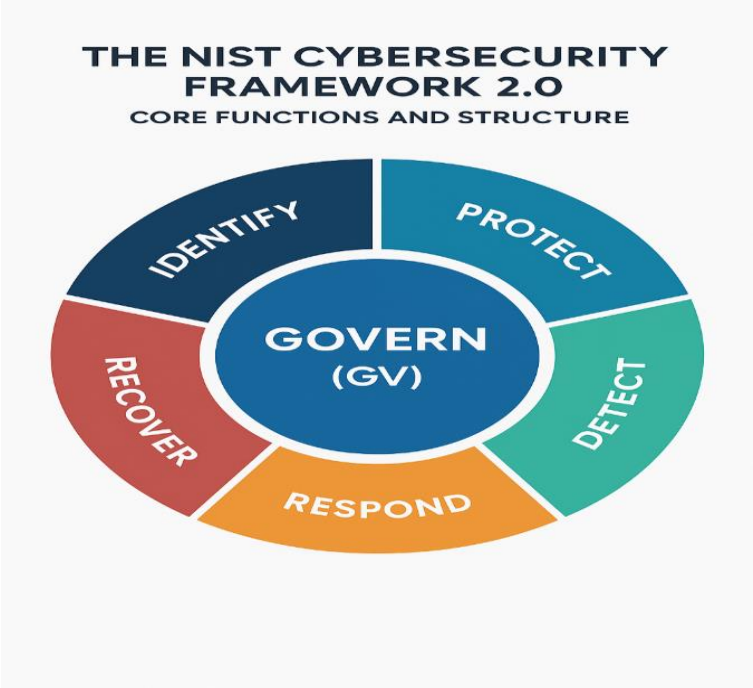

Figure 2. The NIST Cybersecurity Framework 2.0 Core Functions and Structure (NIST, 2024)

Effective strategic leadership must mandate the use of internationally recognised, adaptable security frameworks like the CSF. This visual aid clarifies the hierarchical nature of the Functions, emphasising that **GOVERN** is central to all other activities.

RESULT AND DISCUSSION

Operationalizing Readiness through Strategic Frameworks

The systematic approach to readiness is dictated by frameworks that translate strategic intent (governance) into operational security (PwC, 2026). The NIST CSF 2.0 provides the comprehensive structure, with **Govern** functioning as the nucleus, informing how the organisation implements the other five functions in the context of its mission and stakeholder expectations (NIST, 2024).

Building on this foundational structure, strategic leaders must mandate specific, high impact security actions to maximise risk reduction. The Cross Sector Cybersecurity Performance Goals (CPGs), developed by CISA based on operational data, serve as this actionable mandate (CISA, n.d. a). Key leadership directives derived from the CPGs include:

Accountability and Asset Inventory: Leaders must formally name a specific accountable role for overall cybersecurity activities and a separate accountable role for Operational Technology (OT) specific cybersecurity (CISA, n.d. a). Furthermore, a continuously updated inventory of all Information Technology and OT assets with IP addresses is required to manage vulnerabilities effectively (CISA, n.d. a; StrongBox IT, 2025).

Vulnerability Management: All known exploited vulnerabilities (KEVs) on internet facing systems must be patched or mitigated within a risk informed span of time, prioritising critical assets (CISA, n.d. a). For OT

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XII, December 2025

systems where patching risks availability or safety, compensating controls such, as network segmentation and continuous monitoring, must be applied and recorded (CISA, n.d. a).

Access Control: Phishing resistant Multifactor Authentication is critical for accounts with remote access (CISA, n.d. a). Organisations must enforce a system mandated policy that requires a minimum password length of fifteen or more characters (CISA, n.d. a). Administrators must maintain separate user accounts for non administrative activities, ensuring no user account always possesses super user privileges (CISA, n.d. a).

Adversarial Testing: Readiness must be validated through rigorous, independent third-party exercises (CISA, n.d. a). These exercises must explicitly consider "assume breach" scenarios, testing the adversary's ability to pivot laterally and compromise critical systems (CISA, n.d. a).

The Discussion on Financial Accountability and Incentives

Cyber risk quantification facilitates strategic resource allocation by clarifying risk in monetary terms (SecurityScorecard, 2025a; Balbix, 2025). This capacity is leveraged to manage accountability at the executive level. Monetary penalties tied directly to cyber incidents have emerged as an effective mechanism to compel CEOs and senior executives to treat cyber risk as a core strategic issue (Turgal, 2025). For example, boards have demonstrated a willingness to reduce short term compensation for the CEO and executive team in response to major cyberattacks that significantly disrupted customers (Turgal, 2025).

While boards maintain discretionary powers and clawback provisions to address failures retrospectively, strategic leadership should focus on proactive incentives (WTW, 2025). Tying executive compensation, particularly annual bonuses, to measurable, forward looking security metrics, such as improvement in CRQ scores or reduction in Mean Time to Detect, reinforces strategic investment and drives preemptive risk reduction behaviour (WTW, 2025). Since the unpredictable nature of cyber events makes predefining formulaic measures challenging, the board’s business judgment remains paramount in determining the appropriate compensation response (WTW, 2025).

Strategic Mitigation of Systemic Resilience Gaps

Managing the Extended Enterprise and Supply Chain Risk

Digital transformation expands the organisation’s attack surface by increasing dependencies on third parties and vendors, making the extended enterprise a major source of systemic risk (Principles for Board Governance of Cyber Risk, 2021). Attacks across the supply chain can infiltrate a system through an outside provider, exploiting a vendor’s weak security controls (The Institute for Defense and Business, 2025).

Strategic leaders must formalise supply chain security through rigorous contractual mandates (CISA, n.d. a). Procurement documents and contracts must explicitly stipulate that vendors notify the customer of confirmed security vulnerabilities in their assets and report security incidents within a risk informed time frame (CISA, n.d. a). Furthermore, vendor selection processes should systematically evaluate and prefer the more secure offering and supplier when cost and function are otherwise similar, thereby reducing risk through better procurement (CISA, n.d. a). Continuous monitoring of vendor security performance is also critical, moving beyond traditional point in time assessments (BitSight Technologies, 2023; SecurityScorecard, 2025c).

Addressing the Talent Gap and Technical Debt

The chronic shortage of skilled cybersecurity professionals is a critical vulnerability that increases organizational exposure (PwC, 2026). Strategic mitigation demands innovative solutions beyond traditional hiring. Forward thinking organizations are leveraging agentic Artificial Intelligence systems to automate continuous control validation, reducing reliance on scarce human analysts and providing cryptographic proof of control efficacy (PwC, 2026).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XII, December 2025

While agentic Artificial Intelligence can reduce dependence on scarce cybersecurity talent, it also introduces new governance and risk considerations. Automated systems may expand the organisational attack surface, suffer from model drift, or generate opaque decisions that are difficult to audit. Without clear accountability and human oversight, automation may amplify rather than reduce systemic risk. Strategic leaders must therefore mandate human in the loop governance, periodic model validation, and explicit ownership of AI driven security decisions.

Concurrently, leaders must address technical debt, which refers to the costs incurred by taking shortcuts in technology infrastructure that result in outdated, vulnerable systems (CISA, n.d. d). Prioritising the retirement or hardening of these systems must be guided by Cyber Risk

Quantification to ensure resources are allocated where they reduce the most significant potential financial exposure (Balbix, 2025). Institutionalising "Secure by Design" principles by mandating Architecture and Engineering Review Boards to vet all technical designs prevents the accumulation of new debt and ensures security is built in from the foundation (CISA, n.d. d).

Although this study draws primarily on US based frameworks, the proposed leadership model is adaptable across jurisdictions and sectors. In the European Union, regulatory regimes such as the NIS2 Directive and the Digital Operational Resilience Act impose more prescriptive governance and reporting obligations, particularly within financial services. In heavily regulated sectors such as finance and healthcare, the relationship between executive accountability, governance maturity, and cyber readiness is likely to be stronger due to regulatory enforcement and supervisory scrutiny.

CONCLUSION AND IMPLICATIONS FOR THEORY AND PRACTICE

This paper set out to reconceptualise cybersecurity readiness as an outcome of strategic leadership rather than a function of technical maturity or compliance adherence alone. In digitally transforming organisations, cyber risk has become a material enterprise risk whose effective management depends on executive accountability, governance coherence, and financially informed decision making. By integrating these elements into a single causal framework, this study advances existing literature that has largely treated governance, risk quantification, and operational frameworks as parallel rather than interdependent domains.

The Strategic Cyber Leadership Model developed in this paper explains how distributed C suite accountability serves as the primary leadership input shaping cybersecurity outcomes. When accountability is concentrated solely within technical roles, cybersecurity initiatives remain operationally fragmented and strategically underprioritised. In contrast, when accountability is distributed across senior executives, cybersecurity becomes embedded within strategic planning and organisational culture. This theoretical position directly supports Proposition 1, which links executive accountability to improved cyber readiness outcomes.

Cyber Risk Quantification is theorised as the central mechanism translating leadership intent into actionable investment decisions. By expressing cyber exposure in financial terms, CRQ aligns cybersecurity decision making with established enterprise risk and capital allocation processes. This mediating role, articulated in Proposition 2, explains why organisations with similar technical environments often display markedly different readiness outcomes depending on whether leadership decisions are informed by financialised risk signals rather than qualitative assessments alone.

The model further posits that integration of cyber risk into Enterprise Risk Management amplifies the effectiveness of CRQ. When cyber risk is assessed alongside operational, financial, and strategic risks, it benefits from established governance routines, escalation thresholds, and board oversight mechanisms. This governance amplification effect underpins Proposition 3 and helps explain why cyber initiatives gain durability when embedded within ERM rather than managed as standalone security programmes.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XII, December 2025

Contextual moderators play a critical role in shaping these relationships. Regulatory intensity strengthens the linkage between governance maturity and cybersecurity readiness by increasing executive exposure to accountability mechanisms, thereby reinforcing Proposition 4. Similarly, the degree of digital transformation intensifies cyber dependency and expands attack surfaces, magnifying the impact of strategic leadership on readiness outcomes as articulated in Proposition 5. These contextual effects clarify why uniform adoption of frameworks does not yield uniform resilience across organisations or sectors.

From a theoretical perspective, this study contributes to cybersecurity and strategic management scholarship by offering a leadership centred explanation of readiness outcomes. It shifts the analytical focus away from control inventories and maturity checklists towards organisational decision structures, incentive mechanisms, and governance processes. The proposed propositions provide a foundation for future empirical research using survey methods, archival risk data, or longitudinal case studies to test the causal pathways articulated in the model.

From a practical perspective, the findings underscore that sustained cybersecurity readiness cannot be achieved through technical excellence alone. Boards and senior executives must institutionalise accountability, mandate financially grounded risk assessment, and ensure that cybersecurity governance is integrated into enterprise-wide decision making structures. While frameworks such as NIST CSF 2.0 and the CISA Cybersecurity Performance Goals provide essential operational guidance, their effectiveness ultimately depends on the quality of strategic leadership that governs their implementation.

In conclusion, cybersecurity readiness should be understood as a leadership capability embedded within organisational governance rather than a technical attribute of information systems. By articulating the mechanisms through which executive accountability, risk financialisation, and governance integration jointly shape resilience, this paper offers a conceptual foundation for both scholarly inquiry and executive action in an increasingly digitised risk environment.

REFERENCE

1. Aon (2025). Integrating cyber risk into ERM: A guide for leaders. Retrieved on 11 October, 2025, from Aon website: https://www.aon.com/en/insights/articles/integrating-cyber-risk-into-erm-a-guide-for-leaders
2. Balbix (2025). What is Cyber Risk Quantification?. Retrieved on 25 July, 2025, from Balbix website: https://www.balbix.com/insights/what-is-cyber-risk-quantification/
3. BitSight Technologies (2023). Cybersecurity readiness: 4 evaluation steps. Retrieved on 13 September, 2025, from BitSight Technologies website: https://www.bitsight.com/blog/cybersecurity-readiness
4. CISA (n.d.). Cybersecurity best practices. Retrieved on 2 November, 2025, from Cybersecurity and Infrastructure Security Agency website: https://www.cisa.gov/topics/cybersecurity-best-practices
5. CISA (n.d.). Cybersecurity governance. Retrieved on 28 November, 2025, from Cybersecurity and Infrastructure Security Agency website: https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance
6. CISA (n.d.). Cybersecurity performance goals (CPGs). Retrieved on 11 August, 2025, from Cybersecurity and Infrastructure Security Agency website: https://www.cisa.gov/cybersecurity-performance-goals-cpgs
7. CISA (n.d.). Executives. Retrieved on 10 September, 2025, from Cybersecurity and Infrastructure Security Agency website: https://www.cisa.gov/audiences/executives
8. Complyance (2025). Aligning cybersecurity with business objectives: A CISO's guide. Retrieved on 3 November, 2025, from Complyance website: https://www.complyance.com/resources/aligning-cybersecurity-with-business-objectives-a-cisos-guide
9. DNV (n.d.). Align cybersecurity strategy with business goals. Retrieved on 11 September, 2025, from DNV website: https://www.dnv.com/cyber/challenges/strategy/
10. FS-ISAC (2021). If cyber is material, then boards are accountable. Retrieved on 1 August, 2025, from FS-ISAC website: https://www.fsisac.com/insights/if-cyber-is-material-then-boards-are-accountable

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XII, December 2025

11. Harvard Law School Forum on Corporate Governance (2021). Principles for board governance of cyber risk. Retrieved on 7 July, 2025, from Harvard Law School Forum on Corporate Governance website: https://corpgov.law.harvard.edu/2021/06/10/principles-for-board-governance-of-cyber-risk/
12. NIST (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
13. PwC (2026). What's important to the CISO in 2026. Retrieved on 30 September, 2025, from PwC website: https://www.pwc.com/us/en/executive-leadership-hub/ciso.html
14. SecurityScorecard (2025a). Cyber risk quantification. Retrieved on 27 October, 2025, from SecurityScorecard website: https://securityscorecard.com/platform/cyber-risk-quantification/
15. SecurityScorecard (2025b). How to communicate third-party risk to the board. Retrieved on 29 October, 2025, from SecurityScorecard website: https://securityscorecard.com/blog/how-to-communicate-third-party-risk-to-the-board/
16. SecurityScorecard (2025c). Cyber Risk Quantification for Financial Risk Reduction. Retrieved on 9 October, 2025, from SecurityScorecard website: https://securityscorecard.com/blog/cyber-risk-quantification-for-financial-risk-reduction/
17. StrongBox IT (2025). Cybersecurity responsibilities across the C suite: A breakdown for every executive. Retrieved on 26 September, 2025, from StrongBox IT website: https://www.strongboxit.com/cybersecurity-responsibilities-across-the-c-suite/
18. The Institute for Defense and Business (2025). The role of cybersecurity in supply chain management. Retrieved on 14 September, 2025, from The Institute for Defense and Business website: https://www.idb.org/the-role-of-cybersecurity-in-supply-chain-management/
19. Turgal, J. (2025). The rise of compensation linked consequences following a breach. SC Media. Retrieved on 2 August, 2025, from https://www.scworld.com/perspective/the-rise-of-compensation-linked-consequences-following-a-breach
20. WTW (2025). Incentive compensation and cybersecurity: What's the connection?. Retrieved on 20 August, 2025, from WTW website: https://www.wtwco.com/en-us/insights/2025/10/incentive-compensation-and-cybersecurity-whats-the-connection