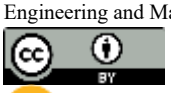
The Role of Cybersecurity in Organizational Strategy and Corporate Governance

1. Lakshmi T
MBA, Department of Management Studies, CMR Institute of Technology, Bengaluru
2. Khushi K R
MBA, Department of Management Studies, CMR Institute of Technology, Bengaluru

How to Cite this Article:
T, L. & R, K. K. (2026). The Role of Cybersecurity in Organizational Strategy and Corporate Governance. International Journal of Creative and Open Research in Engineering and Management, 02(7). https://doi.org/10.55041/ijcope.v2i7.099



https://doi.org/ 10.55041/ijcope.v2i7.099

ABSTRACT

This study examines the evolving role of cybersecurity in organizational strategy and corporate governance, moving beyond its traditional treatment as a purely technical, IT-level concern. Primary data was collected from 50 respondents across finance, healthcare, telecommunications, and technology sectors through a structured questionnaire, using a convenience sampling technique, supplemented by secondary data from organizational reports, academic journals, and case studies. The findings reveal that while cybersecurity awareness exists among employees, it remains inconsistent across roles and organizations, with weak passwords and lack of training identified as the most significant vulnerabilities. Foundational tools such as antivirus software, data encryption, and multi-factor authentication are widely adopted, but more advanced defences like intrusion detection systems remain underutilized. The study further finds that strategic integration of cybersecurity into governance frameworks is limited, with board-level and senior management involvement still insufficient in many organizations. Confidence in an organization's ability to recover from a cyberattack is only moderate, pointing to gaps in incident response and business continuity planning. The study concludes that cybersecurity must be repositioned from a technical function to a strategic, board-level priority, requiring stronger leadership involvement, continuous training, and more robust risk management frameworks.

KEYWORDS

Cybersecurity Governance, Corporate Governance, Organizational Strategy, Risk Management, Cybersecurity Awareness, Board-Level Oversight, Regulatory Compliance

1. INTRODUCTION

In today's digital era, cybersecurity plays a crucial role in shaping organizational strategy and corporate governance. As businesses increasingly rely on digital technologies, protecting sensitive information has become a top priority. Cyber threats are no longer merely an IT issue; they have escalated to a governance and strategic level, requiring board members and executives to take an active role in cybersecurity decision-making. Corporate governance frameworks must integrate cybersecurity policies that align with business objectives, ensuring accountability, compliance, and risk management at all levels.

Traditionally, cybersecurity was regarded as a technical concern delegated to IT departments. This perception has changed as cyber risks have become strategic business issues, with modern governance frameworks now recognizing cybersecurity as a key component of enterprise risk management requiring oversight from boards of directors and executive management. This paper explores the changing role of cybersecurity in corporate governance and strategic management, evaluating the incorporation of cybersecurity into strategic planning, the impact of regulatory frameworks, and the responsibilities of corporate leaders in maintaining a robust security posture.

Relevance of the Study

Cybersecurity is at the center of organizational strategy and corporate governance globally, especially given the increasing occurrence and complexity of cyberattacks. Data breaches, ransomware attacks, and cyber-espionage expose corporations to financial losses, reputational damage, and regulatory penalties. Most companies still treat cybersecurity as a purely technological issue, giving limited weight to its strategic dimension. By exploring the relationship between cybersecurity practices, decision-making, regulatory compliance, and risk management, this study offers relevant insights for decision-makers, policy-makers, and IT professionals.

Problem Statement

Despite the exponential rise in cyber threats, many institutions fail to link strategic planning with cybersecurity risk management. Cybersecurity continues to be perceived as a technical matter rather than a business imperative, resulting in weak risk management, regulatory non-compliance, and insufficient leadership oversight. This study examines these gaps and provides insights into the regulatory, leadership, and organizational factors that can help institutions strengthen their security posture.

Objectives of the Study

• To assess the level of cybersecurity awareness among individuals in various organizational roles.

• To evaluate how effectively organizations integrate cybersecurity into their governance and strategic planning.

SL.NO	Citation	Framework	Research Question	Methodology	Major Findings	Conclusion
1	Williams, Hardy & Holgate (2013)	Socio-Technical Systems & Institutional Logics	How do ISG arrangements form in critical infrastructure organizations?	Interpretive case study, 14 Australian organizations	ISG practices vary by internal/external factors; adaptable models preferred over standardized ones	ISG should be reframed as Information Protection Governance
2	Mears & von Solms	Corporate Governance Strategy	How does governance reinforce cybersecurity?	Conceptual analysis	Security governance is a board-level matter, not solely IT	Cybersecurity needs board oversight and formal governance
3	Tan, Ruighaver & Ahmad (2010	Security Governance & Compliance	Does compliance override effective security?	Case study, multinational firm	Centralized governance restricts flexibility and responsiveness	Decentralized model needed across all level
4	Ako-Nai & Singh (2019)	IT Governance & Contingency Theory	How does board-level IT governance affec performance?	Semi-structured interviews, 10 JSE-listed firms	IT governance often delegated away from the board	Direct board involvement is essential
5	HOT Theory study (2020)	Human-Organization-Technology	What drives cybersecurity effectiveness?	Survey of 151 professionals	Legal and technical controls are strongest predictors	Integrate technical, managerial and legal elements
6	Makari (2020	TPB, DOI, TAM TOE	What drives adoption of IS innovations?	Theoretical model development	Compliance, controls and management commitment drive adoption	Align technology, policy and regulation
7	Gwala & Mashau (2022)	Agency, RBV, Stakeholder, Contingency	Effect of governance on performance in 4IR?	Systematic review, 42 articles	Governance positively affects firm performance	Governance must evolve with technology
8	McFadzean, Ezingeard & Birchall (2007)	Constructivist Grounded Theory	How do boards perceive security risk?	43 executive interviews, 29 organizations	Board involvement depends on perceived risk	Greater board involvement improves planning
9	Schinagl & Shahim (2020	Digital Security Governance Model	How has ISG evolved digitally	Systematic literature review	Conventional ISG inadequate for dynamic environments	Business-integrated security

SL.NO	Citation	Framework	Research Question	Methodology	Major Findings	Conclusion
						frameworks needed
10	Gashgari, Walters & Wills (2017)	ISO/IEC 27014 & COBIT 5	What are CSFs for ISG?	Literature review & framework development	17 critical success factors identified	ISG must be part of corporate governance

• To examine the extent to which technological tools and regulatory compliance are implemented for cybersecurity.

• To explore the types of cybersecurity tools commonly adopted by organizations.

• To measure confidence levels in an organization's ability to recover from cyberattacks.

2. REVIEW OF LITERATURE

Cybersecurity governance refers to the systems, policies, and practices implemented to manage cybersecurity risks within an organization. The literature draws on multiple theoretical lenses including Agency Theory, Resource-Based View, Strategic Alignment Theory, Risk Management Theory, Stakeholder Theory, and the Technology Acceptance Model to explain how organizations align cybersecurity with governance and strategic objectives.

Research Gap

• Limited board-level engagement in cybersecurity, with most organizations still viewing it as an IT concern.

• Insufficient balance between regulatory compliance and proactive, risk-driven cybersecurity strategies.

• Lack of industry-specific cybersecurity governance frameworks for sectors such as healthcare, finance, and critical infrastructure.

• Limited research on the impact of emerging technologies (AI, blockchain, IoT) on cybersecurity governance.

• Few studies quantify the financial and ROI impact of cybersecurity investment on business governance.

3. RESEARCH METHODOLOGY

The study adopts a quantitative descriptive research design aimed at understanding how cybersecurity is integrated into organizational operations, strategic planning, and governance. Descriptive research enables exploration of relationships between variables such as cybersecurity integration, governance structures, and strategic decision-making without manipulating them.

Objectives

1. Assess cybersecurity awareness across organizational roles.

2. Evaluate integration of cybersecurity into governance and strategic planning.

3. Examine implementation of technological tools and regulatory compliance.

4. Explore commonly adopted cybersecurity tools.

5. Measure confidence in an organization's ability to recover from cyberattacks.

Sample Size: 50 respondents, drawn from finance, healthcare, telecommunications, and technology sectors.

Sampling Technique: Convenience Sampling.

Tools Used: Google Forms, Microsoft Excel, Google Sheets — percentage analysis, Likert scale analysis, bar and pie charts.

4. DATA ANALYSIS AND INTERPRETATION

Table 4.1 Demographic Profile of Respondents

Variable	Category	Percentage (%)
Gender	Female	54
Gender	Male	46
Age	21-25 years	76
Age	Below 20	12
Age	26-30	10
Education	Postgraduate	52
Education	Undergraduate	46

Interpretation: The majority of respondents are female (54%), aged 21-25 (76%), and hold postgraduate qualifications (52%), indicating a well-educated, early-career respondent base.

Table 4.2 Cybersecurity Awareness and Practices

Variable	Key Result
Regular cybersecurity awarenes training	38% agree, 34% neutral, 28% disagree
Awareness of cybersecurity policie	Moderate awareness; 30% neutral, 30% agree
Risk management addresses cybe threats	54% agree/strongly agree, 24% disagree
Frequency of cybersecurity audits	44% sometimes; only 38% often/always
Primary responsibility fo cybersecurity	34% Security Team, 26% IT Department, 22% Senio Management

Interpretation: Cybersecurity awareness and governance practices exist but are inconsistent, with senior management involvement notably lower than that of technical teams.

Table 4.3 Cybersecurity Tools Adopted

Tool	Percentage (%)
Data Encryption	46
Antivirus Software	44

Tool	**Percentage (%)**
Multi-Factor Authentication	42
Firewalls	28
Intrusion Detection Systems	18

Interpretation: Foundational tools dominate adoption, while advanced defenses such as intrusion detection systems remain underutilized, indicating room to strengthen technical depth.

Table 4.4 Vulnerabilities and Recovery Confidence

Category	**Top Result**
Most vulnerable area	Weak passwords (54%), Lack of training (42%)
Confidence in recovering from a cyberattack	46% moderately confident, 32% slightly confident, 12% no confident

Interpretation: The human factor — weak passwords and inadequate training — is the leading vulnerability, and confidence in incident recovery capability remains only moderate across organizations.

5. RESULTS AND DISCUSSION

The findings indicate that cybersecurity awareness, while present, is not uniformly embedded across organizational roles. A significant share of respondents remain neutral or uncertain about existing policies and training efforts, pointing to communication gaps between security teams and the broader workforce. Weak passwords and insufficient training emerge as the leading human vulnerabilities, reinforcing the view that technical safeguards alone cannot compensate for gaps in security culture.

Strategic integration of cybersecurity into governance remains limited: senior management involvement lags behind that of dedicated IT and security teams, and cybersecurity audits are conducted inconsistently. This aligns with the literature's recurring theme that cybersecurity is still largely delegated rather than treated as a board-level strategic priority. Foundational technical tools antivirus software, encryption, and multi-factor authentication are widely used, but the underutilization of advanced tools such as intrusion detection systems reflects limited technological maturity in many organizations. Moderate confidence in recovery capability further underscores the need for stronger incident response and business continuity planning.

6. KEY FINDINGS

1. Cybersecurity awareness exists but is inconsistent across organizational roles.

2. Weak passwords and lack of training are the most significant vulnerabilities.

3. Strategic integration of cybersecurity into governance is limited; senior leadership involvement is comparatively low.

4. Foundational tools (antivirus, encryption, MFA) are widely adopted; advanced tools like IDS are underutilized.

5. Cybersecurity audits are conducted inconsistently across organizations.

6. Confidence in recovering from a cyberattack is only moderate, indicating gaps in incident response readiness.

7. RECOMMENDATIONS

1. Implement continuous, mandatory cybersecurity awareness training covering password hygiene and phishing recognition.
2. Integrate cybersecurity into core strategic planning rather than treating it as an isolated IT function.
3. Promote active executive and board-level involvement in cybersecurity decision-making.
4. Invest in advanced security tools such as intrusion detection systems, SIEM, and EDR technologies.
5. Strengthen incident response and disaster recovery planning through regular testing.
6. Enforce strong password policies and multi-factor authentication to address human vulnerabilities.
7. Increase the frequency and rigor of cybersecurity audits and risk assessments.
8. Ensure ongoing compliance with cybersecurity standards such as ISO 27001, NIST, and GDPR.
9. Allocate a dedicated cybersecurity budget covering infrastructure, training, and compliance.

8. SCOPE FOR FUTURE RESEARCH

Future research could explore longitudinal changes in cybersecurity maturity, industry-specific comparisons across healthcare, finance, and manufacturing sectors, the impact of board-level cybersecurity committees on governance outcomes, and cost-benefit or ROI analysis of cybersecurity investment. Qualitative studies examining organizational culture and behavioural factors, along with cross-geographic comparisons of regulatory and governance environments, would further deepen understanding of this evolving field.

9. CONCLUSION

This study confirms that cybersecurity has evolved from a purely technical concern into a strategic, organization-wide priority. While awareness and foundational protective measures are reasonably established, meaningful integration of cybersecurity into corporate governance and strategic decision-making remains inconsistent, particularly at the board and senior leadership level. The human factor reflected in weak passwords and insufficient training stands out as the most pressing vulnerability, while moderate confidence in recovery capability highlights the need for stronger incident response frameworks. Going forward, organizations must treat cybersecurity as a core governance imperative, supported by leadership commitment, continuous risk assessment, and sustained investment in both technology and people.

10. REFERENCES

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., ... & Savage, S. (2019). Security economics and the internal market. European Network and Information Security Agency (ENISA).

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), 69–104.

ENISA. (2023). Threat Landscape Report 2023. European Union Agency for Cybersecurity.

Kaspersky Lab. (2022). IT Security Economics Report.

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Williams, Hardy & Holgate (2013). Information Security Governance in critical infrastructure organizations.

Mears, L., & von Solms, R. Corporate Information Security Governance.

Tan, T., Ruighaver, A. B., & Ahmad, A. (2010). Information security governance: When compliance becomes more important than security.

Ako-Nai, A., & Singh, A. M. (2019). IT governance practices and organizational performance.

Makari, J. (2020). Adoption of Information Security innovations: An integrated theoretical model.

Gwala, R., & Mashau, P. (2022). Corporate governance and organizational performance in the Fourth Industrial Revolution: A systematic review.

McFadzean, E., Ezingeard, J. N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy.

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? From the basement to the boardroom.

Gashgari, G., Walters, R. J., & Wills, G. (2017). A proposed best-practice framework for information security governance.