International Journal of Advanced Engineering and Management Research

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Translating Cybersecurity for Executive Decision-making: Bridging Technical Risk and Board-level Governance in Healthcare Organizations

Dr. Gilbert B. Mengnjo (Co-Lead Author), Dr. Robb Shawe (Co-Lead Author)
Department of Critical Infrastructure, Capitol Technology University, 11301 Springfield Road, Laurel, MD, USA

doi.org/10.51505/ijaemr.2026.11309 URL: http://dx.doi.org/10.51505/ijaemr.2026.11309

Received: Apr 23, 2026 Accepted: Apr 29, 2026 Online Published: May 19, 2026

Abstract
This article examines the challenges associated with translating cybersecurity risk into executive-level decision-making within healthcare organizations. While cybersecurity operations generate significant technical data and insights, these outputs are often not effectively communicated to support strategic governance and board oversight. This study adopts a conceptual governance analysis, informed by evidence from organizational cases, to explore the disconnect between technical cybersecurity reporting and executive decision-making processes. The findings indicate that gaps in translation can lead to misaligned priorities, insufficient risk awareness, and ineffective governance. The article introduces an executive cybersecurity translation model and provides practical implications for improving the alignment of communication, reporting, and decision-making between cybersecurity functions and organizational leadership.

Keywords: cybersecurity governance; executive decision-making; board oversight; risk communication; healthcare cybersecurity; enterprise risk management

1. Introduction

1.1 Background of the Problem

Cybersecurity has become a critical organizational risk that requires attention at the highest levels of leadership. In healthcare organizations, cyber risks affect patient safety, data privacy, regulatory compliance, and operational continuity. As a result, boards of directors and executive leaders are increasingly expected to oversee cybersecurity as part of enterprise risk management (Behl & Behl, 2017; Whitman & Mattord, 2017).

However, cybersecurity remains a technically complex domain, often communicated through metrics, logs, and system-level indicators that are not easily interpretable by non-technical stakeholders. This creates a disconnect between cybersecurity operations and executive decision-making.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

This article is part of the Mengnjo–Shawe research series, which examines cybersecurity governance in healthcare organizations through an integrated analytical framework encompassing outsourcing risk, human factors, socio-technical systems, regulatory alignment, and organizational decision-making.

1.2 Problem Statement

Despite the growing importance of cybersecurity governance, organizations frequently struggle to translate technical cybersecurity data into meaningful information for executive decision-making. This translation gap limits leadership's ability to assess risk, prioritize investments, and exercise effective oversight. In healthcare settings, where regulatory and operational stakes are high, this gap can undermine governance effectiveness and organizational resilience.

1.3 Purpose of the Article

The purpose of this article is to examine how cybersecurity information can be translated into formats that support executive decision-making and governance in healthcare organizations.

1.4 Research Questions

RQ1: How is cybersecurity information currently communicated to executive leadership?

RQ2: What challenges exist in translating technical cybersecurity data into governance-relevant insights?

RQ3: How can organizations improve cybersecurity risk communication for executive decision-making?

1.5 Contribution to the Literature

This article contributes to the literature by proposing a structured governance mechanism to translate technical cybersecurity data into executive-level decision-making frameworks. Specifically, it introduces a conceptual translation model that connects operational cybersecurity metrics to business risk, strategic priorities, and board-level oversight.

The study further advances cybersecurity governance literature by conceptualizing risk translation as a formal governance process rather than a purely technical reporting activity.

By addressing the persistent disconnect between technical reporting and executive understanding, this study extends existing cybersecurity governance and enterprise risk management (ERM) literature through a decision-centric lens that emphasizes communication, interpretation, and actionability.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

1.6 Series Integration and Positioning

This study builds upon prior analyses of outsourcing (Article 1), human factors (Article 2), socio-technical integration (Article 3), organizational structure (Article 4), and regulatory alignment (Article 5) by focusing on executive-level governance. Within the Mengnjo–Shawe Series, this article serves as the bridge between operational cybersecurity and strategic decision-making, translating technical, human, and regulatory insights into governance-relevant frameworks for leadership.

2. Literature Review

2.1 Cybersecurity Governance and Executive Oversight

Cybersecurity governance requires active involvement from executive leadership and boards of directors. Whitman and Mattord (2017) emphasized that leadership must ensure alignment between cybersecurity practices and organizational objectives.

Recent research further emphasizes that cybersecurity governance increasingly requires executive-level interpretation of technical risk within broader organizational and operational contexts, particularly in complex healthcare environments (Sarker, 2021).

2.2 Enterprise Risk Management (ERM)

Enterprise risk management frameworks provide a structured approach for integrating cybersecurity into organizational decision-making (Behl & Behl, 2017). ERM emphasizes risk identification, assessment, and communication at the executive level.

2.3 Risk Communication Challenges

Technical cybersecurity data is often complex and difficult to interpret. Nicho (2018) highlighted the importance of governance processes that translate technical information into actionable insights for decision-makers.

Contemporary governance research also highlights that cybersecurity communication failures may emerge when technical reporting lacks organizational context, strategic prioritization, or business-oriented risk framing (Von Solms & Von Solms, 2018).

2.4 Organizational Context

In healthcare organizations, cybersecurity risks intersect with regulatory compliance, patient safety, and operational continuity. Case evidence suggests that limited internal expertise and reliance on external providers can complicate communication between technical teams and leadership.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

2.5 Literature Gap

Existing research has not sufficiently addressed how cybersecurity information can be effectively translated into executive-level decision-making frameworks.

3. Theoretical Framework

This study integrates:

- Enterprise Risk Management (ERM)
- Cybersecurity Governance Theory
- Organizational Communication Theory

These frameworks support analysis of how cybersecurity risk can be translated into decision-relevant information.

4. Methodological Orientation

This study employs a qualitative conceptual governance analysis informed by the cybersecurity governance literature, enterprise risk management frameworks, organizational communication theory, and case-informed evidence from healthcare cybersecurity environments. The analytical process incorporates thematic synthesis techniques commonly used in conceptual governance and organizational communication research to identify recurring patterns in cybersecurity reporting, executive interpretation, governance communication, and strategic decision-making.

Enterprise risk management theory, cybersecurity governance frameworks, and organizational communication theory guided the conceptual analysis. These frameworks were used to examine how technical cybersecurity information is translated into governance-relevant insights within complex healthcare organizations.

Case-informed observations were analytically evaluated through iterative thematic comparison to identify recurring communication gaps between cybersecurity operations and executive leadership. These recurring themes informed the development of the Executive Cybersecurity Translation Model, which conceptualizes cybersecurity communication as a structured governance process that links technical operations to executive oversight and strategic decision-making.

5. Conceptual Model

The Executive Cybersecurity Translation Model

The Executive Cybersecurity Translation Model is developed to address the persistent disconnect between technical cybersecurity operations and executive-level decision-making. In many organizations, cybersecurity functions generate large volumes of technical data, including system

Vol. 11, No. 03; 2026

ISSN: 2456-3676

alerts, vulnerability assessments, and performance metrics. However, these outputs are often not presented in a format that supports strategic interpretation by executive leadership, resulting in a translation gap that limits governance effectiveness.

This model conceptualizes cybersecurity communication as a structured, multi-stage transformation process in which technical data is progressively translated into governance-relevant insights. Rather than treating cybersecurity reporting as a purely technical function, the model positions translation as a critical governance mechanism that links operational cybersecurity activities to enterprise risk management and executive oversight. Each stage of the model reflects a shift from technical specificity toward strategic abstraction, enabling decision-makers to interpret cybersecurity risk in terms of business impact, organizational priorities, and regulatory considerations.

The model further emphasizes that effective cybersecurity governance depends not only on the availability of accurate technical data but also on the organization's capacity to interpret, contextualize, and communicate that data in a manner that supports executive action. By structuring the translation process, the model provides a framework to align cybersecurity operations with organizational strategy, improve risk awareness, and enhance the quality of executive decision-making.

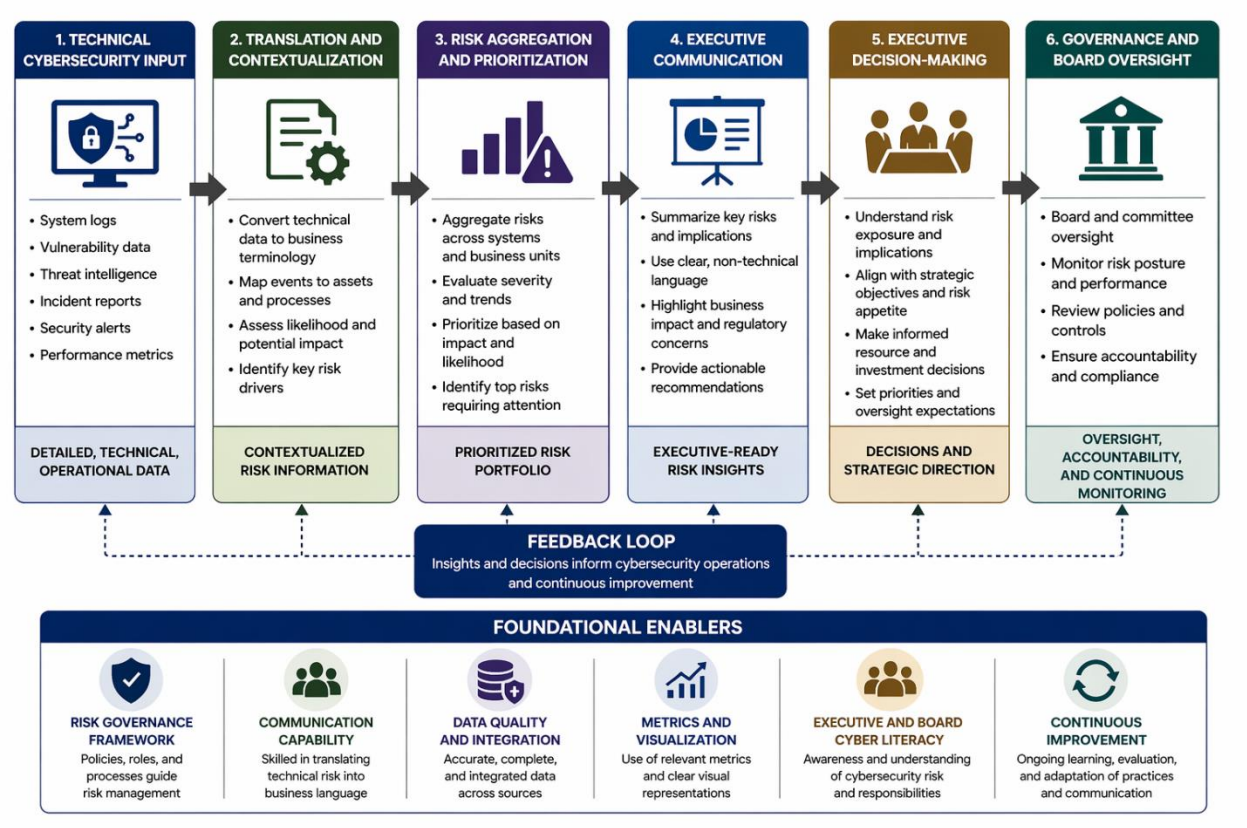
Figure 1 illustrates the process of translating technical cybersecurity information into executive-level decision-making frameworks.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Figure 1

Executive Cybersecurity Translation Model



Note. Author created. The model illustrates how technical cybersecurity data can be translated into governance-relevant insights for executive decision-making.

As illustrated in Figure 1, the effectiveness of cybersecurity governance is not determined solely by the availability of technical data, but by the organization's ability to translate that data into meaningful, decision-relevant insights. The model demonstrates that translation failures can disrupt the flow of information between cybersecurity operations and executive leadership, leading to misaligned priorities, reduced risk awareness, and weakened governance oversight. Conversely, organizations that implement structured translation processes are better positioned to align cybersecurity activities with strategic objectives, enhance executive understanding of risk, and support informed decision-making at the highest levels of governance.

The model highlights that effective cybersecurity governance depends not only on technical capability but on the organization's ability to translate, contextualize, and communicate risk in a manner that supports executive action and strategic oversight.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Key Components of the Model:

- Technical data (alerts, metrics, logs)
- Analytical interpretation
- Risk translation (business impact)
- Executive reporting
- Decision-making and governance action

6. Analytical Discussion

6.1 The Translation Gap

A persistent challenge in cybersecurity governance involves the translation gap between technical cybersecurity operations and executive-level understanding (Nicho, 2018; Behl & Behl, 2017). Although healthcare organizations generate extensive cybersecurity data through monitoring systems, vulnerability assessments, incident-response activities, and security operations centers, this information is frequently communicated in highly technical formats that are not readily interpretable by executive leadership or board members.

Technical cybersecurity reporting often emphasizes system-level metrics such as intrusion attempts, vulnerability scores, patch-management statistics, malware detections, or network anomalies. While these indicators may hold operational significance for cybersecurity professionals, they do not necessarily communicate the organizational implications of risk in terms that support strategic governance or executive decision-making. As a result, executive leaders may struggle to evaluate the significance of cybersecurity threats relative to organizational priorities, regulatory exposure, patient safety, operational continuity, or enterprise risk-management objectives (Whitman & Mattord, 2017).

In healthcare settings, this translation gap may become particularly problematic because cybersecurity risks intersect with clinical operations, patient care delivery, legal obligations, financial stability, and institutional reputation. Technical reports that fail to contextualize cybersecurity risk within these broader organizational dimensions may unintentionally reduce executive awareness of cybersecurity exposure and weaken governance responsiveness.

For example, healthcare cybersecurity teams may report vulnerability-scan results, intrusion alerts, or endpoint-security metrics without clearly explaining how these findings influence operational resilience, patient-care continuity, compliance obligations, or strategic organizational risk. Without structured translation into governance-relevant language, executives may perceive cybersecurity as an isolated technical issue rather than an enterprise-wide governance concern requiring strategic oversight and resource prioritization.

The translation gap may also create communication asymmetries between cybersecurity professionals and executive leadership. Technical teams often possess specialized operational

Vol. 11, No. 03; 2026

ISSN: 2456-3676

knowledge, while executives are responsible for enterprise strategy, governance oversight, and resource allocation. When communication frameworks fail to bridge these differing perspectives, organizations may experience misaligned priorities, fragmented governance coordination, delayed investment decisions, and insufficient organizational preparedness for cybersecurity incidents (Von Solms & Von Solms, 2018).

Accordingly, effective cybersecurity governance requires structured mechanisms to transform technical cybersecurity outputs into governance-oriented insights that support executive interpretation, strategic prioritization, enterprise risk evaluation, and board-level oversight.

6.2 Implications for Risk Awareness

The inability to effectively translate cybersecurity information into executive-relevant terms may significantly weaken organizational risk awareness and governance effectiveness. Executive leadership teams rely upon accurate, contextualized, and actionable information to assess organizational threats, prioritize strategic initiatives, and allocate resources appropriately. When cybersecurity reporting lacks organizational context or strategic interpretation, executives may underestimate the severity, scope, or implications of cybersecurity risk (Behl & Behl, 2017).

One major implication involves resource-allocation challenges. Executives who do not fully understand the scope of cybersecurity exposure may underinvest in critical security infrastructure, workforce development, incident-response capabilities, or governance oversight mechanisms. Conversely, poorly contextualized reporting may also lead organizations to overinvest in highly visible technical controls without adequately addressing broader governance weaknesses or organizational vulnerabilities.

Translation failures may further contribute to distorted risk prioritization. Executive leaders may focus attention on technical metrics that appear operationally significant while overlooking broader systemic issues such as workforce readiness, third-party dependencies, governance fragmentation, or policy implementation gaps. As a result, organizational cybersecurity strategy may become reactive rather than strategically aligned with enterprise risk-management objectives.

In healthcare organizations, limited executive cybersecurity awareness may also influence operational continuity planning and patient-safety preparedness. Cyber incidents in healthcare settings may disrupt clinical systems, compromise patient data, delay treatment delivery, and result in significant legal and regulatory consequences. Without effective governance translation processes, executive leaders may fail to appreciate how cybersecurity disruptions directly affect healthcare operations and institutional resilience (Sarker, 2021).

The findings additionally suggest that inadequate cybersecurity translation may weaken board-level governance oversight. Boards of directors increasingly bear responsibility for cybersecurity governance within enterprise risk-management structures; however, board members often

Vol. 11, No. 03; 2026

ISSN: 2456-3676

possess varying levels of cybersecurity literacy. Governance systems that fail to communicate cybersecurity exposure in strategic and organizational terms may therefore limit the board's ability to exercise informed oversight, evaluate organizational preparedness, or establish risk-governance expectations.

Effective cybersecurity governance consequently requires organizations to establish communication structures that improve executive risk awareness by translating technical cybersecurity conditions into the organizational, operational, regulatory, financial, and strategic implications relevant to leadership decision-making.

6.3 Governance Implications

The findings indicate that cybersecurity governance frameworks must incorporate formal translation mechanisms that bridge technical cybersecurity operations and executive governance structures. Cybersecurity communication should therefore be treated not merely as a reporting activity but as an integrated governance process essential for enterprise risk management, organizational coordination, and strategic decision-making (Nicho, 2018).

Effective governance structures require clear processes for transforming technical cybersecurity information into business-oriented risk insights that align with executive priorities and governance responsibilities. This transformation involves contextualizing technical findings within operational, regulatory, financial, legal, and organizational risk frameworks that executive leadership can meaningfully evaluate and act upon.

The analysis further suggests that governance effectiveness depends upon interdisciplinary coordination among cybersecurity professionals, executive leadership, compliance personnel, operational departments, legal advisors, and enterprise risk-management teams. Without coordinated communication structures, organizations may experience fragmented governance oversight, inconsistent risk interpretation, and reduced organizational alignment regarding cybersecurity priorities.

Governance implications also extend to the design of organizational communication. Healthcare organizations must establish standardized cybersecurity reporting frameworks that support consistency, interpretability, and executive usability. Reporting systems should prioritize clarity, strategic relevance, operational context, and decision-oriented communication rather than relying exclusively on highly technical metrics or isolated operational indicators.

The Executive Cybersecurity Translation Model introduced in this study emphasizes that governance translation involves multiple interconnected stages, including technical interpretation, contextualization, risk prioritization, executive communication, and governance action. Governance breakdowns may occur at any stage of this translation process, thereby disrupting organizational understanding of cybersecurity exposure and weakening executive oversight capacity.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Additionally, governance systems must account for the dynamic nature of cybersecurity risk. Cyber threats evolve rapidly across healthcare environments characterized by interconnected technologies, distributed systems, regulatory complexity, and increasing dependence on digital operations. Governance models that rely upon static or infrequent reporting mechanisms may therefore fail to provide leadership with timely and actionable cybersecurity insight.

The findings further reinforce the importance of integrating cybersecurity governance into enterprise risk-management structures rather than isolating it within technical departments. Governance integration strengthens organizational visibility into systemic vulnerabilities, supports strategic resource allocation, and enhances executive accountability for cybersecurity resilience across the enterprise (Whitman & Mattord, 2017).

Ultimately, the governance implications suggest that healthcare organizations must institutionalize cybersecurity translation as a core governance capability that supports executive interpretation, strategic coordination, organizational resilience, and enterprise-wide risk management.

6.4 Executive Decision-Making

Executive leadership plays a central role in determining how cybersecurity information influences organizational governance, strategic planning, operational resilience, and enterprise risk management. The findings suggest that executives must move beyond passive receipt of cybersecurity reports toward active engagement in governance translation processes that support informed decision-making and organizational oversight (Whitman & Mattord, 2017).

Healthcare executives increasingly operate within environments where cybersecurity risks affect patient safety, regulatory compliance, operational continuity, institutional reputation, and financial stability. Consequently, executive decision-making requires cybersecurity information that is contextualized, strategically relevant, and aligned with organizational priorities rather than limited to technical system outputs alone.

Executives should therefore require structured cybersecurity reporting mechanisms that translate technical indicators into governance-oriented insights. Effective executive reporting should communicate:

- operational impact,
- organizational exposure,
- strategic implications,
- regulatory consequences,
- financial risk,
- and enterprise resilience considerations.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

This structured approach enables leadership teams to prioritize cybersecurity initiatives within broader organizational governance and enterprise risk-management frameworks.

The findings further suggest that executive leadership must foster governance cultures that encourage interdisciplinary communication between technical personnel and organizational leadership. Cybersecurity professionals may possess deep operational expertise, but may not always communicate cybersecurity exposure in language aligned with executive governance processes. Executive leaders should therefore establish communication expectations, governance standards, and reporting structures that facilitate organizational understanding across technical and non-technical stakeholder groups.

Board-level oversight also represents a critical executive consideration. Boards of directors increasingly face expectations to oversee cybersecurity risk as part of enterprise governance responsibilities. Executives serve as the primary interface between cybersecurity operations and board governance, thereby requiring the ability to translate operational cybersecurity conditions into strategic governance discussions appropriate for board-level interpretation.

Additionally, executive decision-making must account for the socio-technical dimensions of cybersecurity governance. Cybersecurity effectiveness is influenced not only by technical infrastructure but also by workforce behavior, organizational communication, policy implementation, operational coordination, and institutional culture. Leadership teams that narrowly frame cybersecurity as a technical issue may overlook broader organizational vulnerabilities that significantly affect cybersecurity resilience.

The analysis therefore indicates that healthcare executives should integrate cybersecurity governance into enterprise strategy development, operational continuity planning, organizational resilience initiatives, and enterprise risk-management processes. Organizations that successfully institutionalize cybersecurity translation mechanisms are better positioned to improve executive risk awareness, strengthen governance coordination, support informed decision-making, and enhance long-term organizational resilience in increasingly complex healthcare cybersecurity environments (Sarker, 2021; Von Solms & Von Solms, 2018).

7. Practical Implications

The findings of this study suggest that healthcare organizations must establish structured governance mechanisms capable of translating technical cybersecurity information into executive-level decision-making frameworks. Effective cybersecurity governance depends not only on the collection of technical security data but also on the organization's ability to contextualize, communicate, and operationalize that information within broader enterprise governance and risk-management processes (Whitman & Mattord, 2017).

Healthcare organizations should therefore develop standardized cybersecurity reporting frameworks designed specifically to support executive interpretation and board-level oversight.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

These frameworks should move beyond purely technical metrics and incorporate governance-oriented indicators that communicate organizational exposure, operational implications, regulatory risk, patient-safety considerations, financial impact, and enterprise resilience.

Organizations should also establish translation protocols that systematically convert technical cybersecurity outputs into business-oriented risk language understandable to executive leadership and non-technical governance stakeholders. Translating cybersecurity data into organizationally relevant terms may improve leadership engagement, strengthen governance coordination, and support more effective strategic prioritization of cybersecurity initiatives.

Executive cybersecurity literacy represents another significant practical implication. Boards of directors and executive leadership teams increasingly bear responsibility for overseeing cybersecurity governance despite varying levels of technical expertise. Healthcare organizations should therefore implement executive-focused cybersecurity education programs that strengthen leadership understanding of cybersecurity concepts, governance responsibilities, enterprise risk exposure, and operational cybersecurity implications (Behl & Behl, 2017).

The findings further suggest that healthcare organizations should integrate cybersecurity governance directly into enterprise risk-management (ERM) structures and strategic governance processes. Cybersecurity should not be treated as an isolated technical function operating independently from organizational leadership. Instead, governance frameworks should incorporate cybersecurity considerations into strategic planning, operational continuity initiatives, compliance management, and enterprise-wide resilience planning.

Organizations may also need to redesign communication processes between cybersecurity professionals and executive leadership. Technical reporting structures that emphasize operational specificity without strategic interpretation may reduce governance effectiveness and limit executive engagement. Accordingly, healthcare organizations should encourage interdisciplinary collaboration among cybersecurity teams, executive leadership, compliance personnel, legal advisors, and enterprise risk-management stakeholders to improve communication consistency and governance integration.

The study also highlights the importance of continuous adaptation in governance. Cybersecurity environments evolve rapidly due to technological innovation, emerging threats, regulatory changes, and organizational transformation. Governance systems should therefore include mechanisms for ongoing reporting refinement, evaluation of communication, integration of executive feedback, and organizational learning to ensure that cybersecurity translation processes remain aligned with evolving operational realities.

Finally, organizations should recognize that effective cybersecurity translation is not solely a communication issue but a governance capability that directly influences executive awareness, resource allocation, risk prioritization, and institutional resilience. Healthcare organizations that

Vol. 11, No. 03; 2026

ISSN: 2456-3676

successfully institutionalize cybersecurity translation processes may improve governance coordination, strengthen strategic oversight, and enhance organizational preparedness in increasingly complex cyber-threat environments.

8. Limitations

This study is subject to several limitations. First, the analysis is conceptual in nature and does not include direct empirical measurement or large-scale quantitative analysis. Although the study integrates cybersecurity governance literature, enterprise risk-management frameworks, organizational communication theory, and case-informed observations, the findings should be interpreted within the context of conceptual governance analysis rather than generalized empirical validation.

Second, the study focuses specifically on healthcare cybersecurity environments, which operate under unique regulatory, operational, and organizational conditions. Consequently, the governance and communication challenges identified may not fully apply to all critical infrastructure sectors or organizational contexts.

Third, the study emphasizes governance translation and executive communication processes rather than technical cybersecurity performance evaluation. While this governance-centered perspective supports examination of organizational and strategic decision-making challenges, it does not evaluate specific cybersecurity technologies, technical architectures, or operational security tools in detail.

Additionally, the case-informed observations referenced throughout the analysis are intended to provide contextual insight into recurring governance and communication challenges rather than represent formal comparative case-study findings. Future empirical research may therefore be necessary to evaluate how cybersecurity translation frameworks operate across diverse organizational structures, leadership environments, and healthcare systems.

The study also does not directly measure executive decision quality, board-level cybersecurity literacy, or organizational governance outcomes associated with cybersecurity translation practices. Accordingly, additional longitudinal and empirical investigation may be necessary to determine how structured translation mechanisms influence the effectiveness of executive governance and enterprise cybersecurity resilience over time.

Despite these limitations, the study contributes meaningful insights into the relationships among cybersecurity communication, executive interpretation, governance integration, and enterprise risk-management processes within healthcare organizations.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

9. Future Research

Future research should empirically evaluate the Executive Cybersecurity Translation Model across diverse healthcare organizations to determine how structured translation mechanisms influence executive decision-making, governance effectiveness, organizational resilience, and enterprise risk-management outcomes. Quantitative and mixed-methods studies may help validate the relationship between cybersecurity translation quality and executive governance performance.

Additional research should examine how executive cybersecurity literacy influences the effectiveness of organizational governance and cybersecurity decision-making. Understanding how leadership knowledge, governance experience, and board-level engagement affect cybersecurity oversight may provide valuable insight into improving executive governance structures within healthcare environments.

Future studies should also explore the relationship between cybersecurity communication practices and organizational resilience outcomes during cyber incidents. Comparative analysis of organizations with differing governance communication structures may help identify translation practices that most effectively support operational continuity, incident-response coordination, and executive preparedness.

Cross-industry comparative research may further clarify how cybersecurity translation challenges differ across sectors such as healthcare, energy, manufacturing, transportation, and financial services. Such analysis may provide insight into sector-specific governance requirements and communication strategies associated with complex cyber-risk environments.
Research examining the influence of emerging technologies—including artificial intelligence (AI), automated reporting systems, predictive analytics, and governance dashboards—may additionally contribute to understanding how organizations can improve executive cybersecurity communication and governance integration in increasingly data-intensive environments (Sarker, 2021).

Future scholarship should also investigate socio-technical dimensions of cybersecurity translation, including organizational culture, workforce communication behavior, interdisciplinary collaboration, leadership trust, and institutional decision-making dynamics. These human-centered governance variables may significantly influence the effectiveness of cybersecurity communication and executive risk interpretation.

Finally, longitudinal research examining how cybersecurity translation processes evolve in response to changing regulatory environments, technological innovation, and emerging cyber threats may help organizations develop more adaptive governance frameworks that support sustained executive oversight and enterprise resilience.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

10. Conclusion

Effective cybersecurity governance within healthcare organizations requires more than technical security operations or compliance-focused reporting mechanisms. As cybersecurity increasingly influences patient safety, operational continuity, regulatory exposure, organizational reputation, and enterprise resilience, healthcare organizations must establish governance structures that translate technical cybersecurity information into executive-level decision-making and strategic oversight processes (Whitman & Mattord, 2017).

The findings indicate that a persistent translation gap exists between cybersecurity operations and executive governance. Technical cybersecurity metrics, system-level indicators, and operational reporting often fail to communicate organizational risk in terms meaningful to executive leadership and boards of directors. This disconnect may contribute to reduced executive risk awareness, fragmented governance coordination, misaligned strategic priorities, and weakened organizational preparedness for cybersecurity incidents (Nicho, 2018).

The Executive Cybersecurity Translation Model introduced in this study conceptualizes cybersecurity communication as a structured governance process rather than a purely technical reporting function. The model demonstrates that effective governance depends on the organization's ability to interpret, contextualize, prioritize, and communicate cybersecurity information in ways that support executive understanding, strategic alignment, enterprise risk management, and board-level oversight.

The study further reinforces that cybersecurity governance is fundamentally socio-technical in nature. Effective executive decision-making depends not only on the availability of technical data but also on communication quality, governance coordination, organizational context, leadership engagement, workforce alignment, and enterprise-wide risk interpretation. Organizations that fail to integrate these dimensions may struggle to align cybersecurity operations with broader institutional objectives and governance responsibilities.

Within the broader Mengnjo–Shawe research series, this article serves as the governance translation bridge connecting operational cybersecurity activities with executive leadership and enterprise governance processes. By integrating technical cybersecurity operations, organizational communication theory, enterprise risk management, and governance oversight, the study advances a governance-centered framework for executive cybersecurity interpretation within complex healthcare environments.

Ultimately, strengthening cybersecurity governance in healthcare organizations requires institutionalizing structured translation mechanisms that connect technical cybersecurity operations to strategic decision-making, executive oversight, and enterprise resilience planning. Organizations capable of effectively translating cybersecurity risk into governance-relevant insight are better positioned to improve leadership awareness, strengthen governance

Vol. 11, No. 03; 2026

ISSN: 2456-3676

accountability, support informed decision-making, and enhance long-term organizational resilience in increasingly complex cyber-threat environments.

Authorship Statement

This research forms part of the Mengnjo–Shawe research series examining cybersecurity governance in healthcare organizations. The foundational empirical insights for this series originate from prior applied research conducted by Dr. Gilbert B. Mengnjo.

Dr. Robb Shawe served as the principal architectural author and governance integrator for the Mengnjo–Shawe Series, leading the conceptual development, methodological structuring, socio-technical synthesis, governance modeling, executive translation frameworks, and series-wide analytical integration across all eight manuscripts. His contributions focused on constructing the unified cybersecurity governance architecture, aligning interdisciplinary theoretical foundations, and ensuring continuity across the program's healthcare cybersecurity governance framework.

Author Note and Copyright Statement

Dr. Gilbert Mengnjo, PhD, MSc

Dr. Gilbert Mengnjo is a cybersecurity governance strategist and risk management leader with more than 15 years of experience guiding enterprise cybersecurity programs across healthcare, manufacturing, global supply chains, and critical infrastructure environments. His expertise includes cybersecurity governance, regulatory compliance, vendor risk management, and security program development aligned with frameworks such as NIST CSF, HIPAA, HITRUST, and ISO 27001.

Dr. Mengnjo contributed practitioner insights, governance analysis, and applied cybersecurity expertise to the conceptual development of the research framework and literature synthesis. His experience translating complex technical risks into operational governance strategies informed the manuscript's analytical perspective.

Dr. Robb Shawe, PhD, MS

Dr. Robb Shawe is a scholar-practitioner, U.S. Navy veteran, and Chief Executive Officer of New York Security Consulting Professionals L.L.C. His research focuses on critical infrastructure protection, cybersecurity governance, organizational resilience, and socio-technical risk management. His scholarship integrates multidisciplinary perspectives spanning cybersecurity, emergency management, occupational health, and sustainability systems.

Dr. Shawe served as the lead author and was primarily responsible for conceptualization, development of the analytical framework, literature synthesis, and manuscript preparation. His work emphasizes the integration of governance structures, resilience systems, and policy

Vol. 11, No. 03; 2026

ISSN: 2456-3676

frameworks designed to strengthen critical infrastructure and organizational security environments.

Conflict of Interest Statement

The authors declare no conflicts of interest related to this research.

Originality Statement

This manuscript represents original scholarly work and is not currently under consideration by another publication outlet.

Copyright Notice

References

Almuhammadi, S., & Alsaleh, M. (2021). Understanding human factors in cybersecurity behavior: A systematic literature review. IEEE Access, 9, 122344–122368.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Behl, A., & Behl, K. (2017). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security*, *26*(1), 10–38.

Sarker, I. H. (2021). Cyberlearning and deep learning-based cybersecurity in healthcare systems. Internet of Things, 14, 100393.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security—What goes where? Information & Computer Security, 26(1), 2–9.

Whitman, M. E., & Mattord, H. J. (2017). *Management of information security* (5th ed.). Cengage Learning.