International Journal of Advanced Engineering and Management Research

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Human Factors in AI-augmented Cybersecurity: Workforce Trust, Usability, and Behavioral Adaptation 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.2026.11305 URL: http://dx.doi.org/10.51505/ijaemr.2026.11305

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

Abstract
This research examines the role of human factors in the effectiveness of AI-augmented cybersecurity systems within healthcare organizations. As organizations increasingly integrate artificial intelligence and automated security tools into their operational environments, workforce interaction with these systems becomes a critical determinant of success. This study adopts a conceptual governance and human-centered analysis, informed by evidence from organizational cases, to explore how trust, usability, and behavioral adaptation influence the implementation and effectiveness of AI-enabled cybersecurity practices. The findings suggest that technical performance alone is insufficient to ensure successful cybersecurity outcomes; rather, workforce perception, organizational culture, and governance structures significantly shape system adoption and operational effectiveness. The study provides a framework for integrating human factors into cybersecurity governance and offers practical implications for healthcare leaders seeking to align technological capability with workforce engagement and organizational oversight.

Keywords: human factors; cybersecurity governance; AI systems; workforce trust; usability; healthcare cybersecurity

1. Introduction

1.1 Background of the Problem

Healthcare organizations are increasingly adopting artificial intelligence (AI) and automated cybersecurity tools to enhance threat detection, monitoring, and response capabilities. These technologies offer substantial improvements in efficiency and scalability, particularly in resource-constrained environments with complex regulatory requirements. However, the effectiveness of these systems is not determined solely by their technical performance. Rather, their success depends significantly on how they are interpreted, trusted, and used by the workforce.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Human interaction with cybersecurity systems plays a central role in determining whether technological capabilities translate into operational effectiveness. Even highly advanced systems may fail to deliver expected outcomes if users do not trust them, misunderstand their outputs, or fail to integrate them into daily workflows.

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 advancements in AI-enabled cybersecurity technologies, organizations continue to experience gaps between system capability and operational effectiveness. A key contributor to this gap is the limited integration of human factors into cybersecurity governance and system design. In healthcare environments, where workflows are complex and time-sensitive, insufficient attention to trust, usability, and behavioral adaptation can undermine the effectiveness of AI-driven cybersecurity systems.

1.3 Purpose of the Article

The purpose of this article is to examine how workforce trust, usability, and behavioral adaptation influence the effectiveness of AI-augmented cybersecurity systems in healthcare organizations.

1.4 Research Questions

RQ1: How does workforce trust influence the effectiveness of AI-enabled cybersecurity systems?

RQ2: What role does system usability play in cybersecurity adoption and operational performance?

RQ3: How do behavioral and organizational factors shape the integration of AI-based cybersecurity tools?

1.5 Contribution to the Literature

This article contributes by:

- Extending cybersecurity research into human-centered and behavioral domains
- Integrating trust and usability into cybersecurity governance frameworks
- Extending socio-technical cybersecurity theory into AI-augmented healthcare governance environments
- Providing organizational insights into AI adoption in healthcare environments

Vol. 11, No. 03; 2026

ISSN: 2456-3676

1.6 Series Integration and Positioning

This study builds upon prior analysis of outsourced cybersecurity governance by examining the human and organizational dimensions that influence the effectiveness of technology-enabled security systems. Within the broader research program, this article focuses on workforce interaction as a critical layer of cybersecurity effectiveness, complementing structural governance analysis by addressing how human behavior, perception, and organizational culture shape system outcomes. By situating human factors within a socio-technical and governance-oriented framework, this study extends beyond technical capability to examine how cybersecurity systems are interpreted, adopted, and operationalized in practice.

2. Literature Review

2.1 Human Factors in Cybersecurity

Human factors play a critical role in the effectiveness of cybersecurity. Organizational behavior, employee attitudes, and user interaction with security systems significantly influence security outcomes. Cuganesan et al. (2018) found that management support and workplace norms shape employee attitudes toward security practices, reinforcing the importance of organizational context in cybersecurity performance.

Recent research further demonstrates that cybersecurity behavior is strongly influenced by organizational awareness programs, workforce education, and human-centered system design (Almuhammadi & Alsaleh, 2021; Aldawood & Skinner, 2020).

2.2 Trust in Technology Systems

Trust is a central determinant of how users interact with automated systems. When users either over-trust or distrust technology, system effectiveness can be compromised. Butavicius et al. (2020) demonstrated that belief in technological controls significantly influences user behavior, sometimes leading to over-reliance or misuse of security systems.

Emerging AI-enabled cybersecurity environments further complicate trust relationships between users and automated systems, particularly when workforce understanding of algorithmic decision-making remains limited (Sarker, 2021).

2.3 Usability and System Interaction

Usability influences whether cybersecurity tools are effectively integrated into operational workflows. Systems that are difficult to interpret or interact with may be ignored, misused, or bypassed. Whitman and Mattord (2017) emphasized that effective security systems must align with user capabilities and organizational processes to ensure adoption and compliance.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

2.4 Socio-Technical Systems Perspective

Socio-technical systems theory highlights the interaction between technology, people, and organizational structures. Carayon (2006) emphasized that system effectiveness depends on the alignment of these elements, particularly in complex environments such as healthcare.

2.5 Governance and Organizational Context

Cybersecurity governance provides the structure through which human factors are integrated into organizational practice. Nicho (2018) emphasized that governance processes must include clear roles, responsibilities, and oversight mechanisms to ensure the system's effective implementation.

2.6 Outsourcing and Third-Party Cybersecurity Context

Although this study focuses on human factors, cybersecurity operations in healthcare environments frequently involve external service providers and technology vendors, particularly in AI-enabled systems. Research on cybersecurity supply chain risk emphasizes that third-party dependencies can introduce governance and operational vulnerabilities when oversight mechanisms are insufficiently integrated into organizational structures (National Institute of Standards and Technology [NIST], 2020; Boyson, 2014). In healthcare environments, these risks are compounded by regulatory requirements and the sensitivity of protected health information, reinforcing the need to align external technological capabilities with internal governance, workforce interaction, and organizational oversight processes (Kruse et al., 2017; Mbonihankuye et al., 2019).

2.7 Literature Gap

While research has examined technical cybersecurity systems and governance structures, little attention has been paid to how human factors—particularly trust, usability, and behavioral adaptation—affect the operational effectiveness of AI-enabled cybersecurity systems in healthcare settings.

3. Theoretical Framework

This study is guided by:

- Socio-Technical Systems Theory (Carayon, 2006)
- Organizational Behavior Theory
- Cybersecurity Governance Frameworks (Nicho, 2018; Whitman & Mattord, 2017)

These frameworks support the integration of human, technical, and organizational dimensions in cybersecurity analysis.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

4. Methodological Orientation

This study employs a qualitative conceptual analysis informed by cybersecurity governance scholarship, human factors research, socio-technical systems theory, and organizational behavior literature associated with AI-enabled operational environments in healthcare organizations. The analytical orientation emphasizes the interaction between human behavior, technological systems, and organizational governance structures to examine how workforce trust, usability, and behavioral adaptation influence cybersecurity effectiveness.

The analytical process incorporated interpretive socio-technical synthesis techniques commonly used in organizational behavior and governance research to evaluate patterns in workforce interaction, system interpretability, behavioral adaptation, operational trust calibration, and the organizational integration of AI-enabled cybersecurity technologies. Socio-technical systems theory, organizational behavior theory, and cybersecurity governance frameworks collectively informed the interpretive analysis of how technological systems influence human decision-making, workforce engagement, and organizational cybersecurity practices.

Case-informed organizational observations were analytically interpreted to identify recurring human-systems interaction patterns affecting cybersecurity implementation, operational integration, and adaptive workforce behavior within complex healthcare environments. These analytical patterns informed the development of the Human–Technology Interaction Model, which conceptualizes how trust, usability, organizational culture, governance oversight, and behavioral adaptation collectively shape cybersecurity effectiveness and organizational resilience.

Although the study does not seek statistical generalizability, the conceptual approach provides a structured interpretive framework for examining the socio-technical relationship between human behavior, organizational governance, and AI-enabled cybersecurity performance in healthcare systems.

5. Conceptual Model

The Human–Technology Interaction Model for Cybersecurity Effectiveness

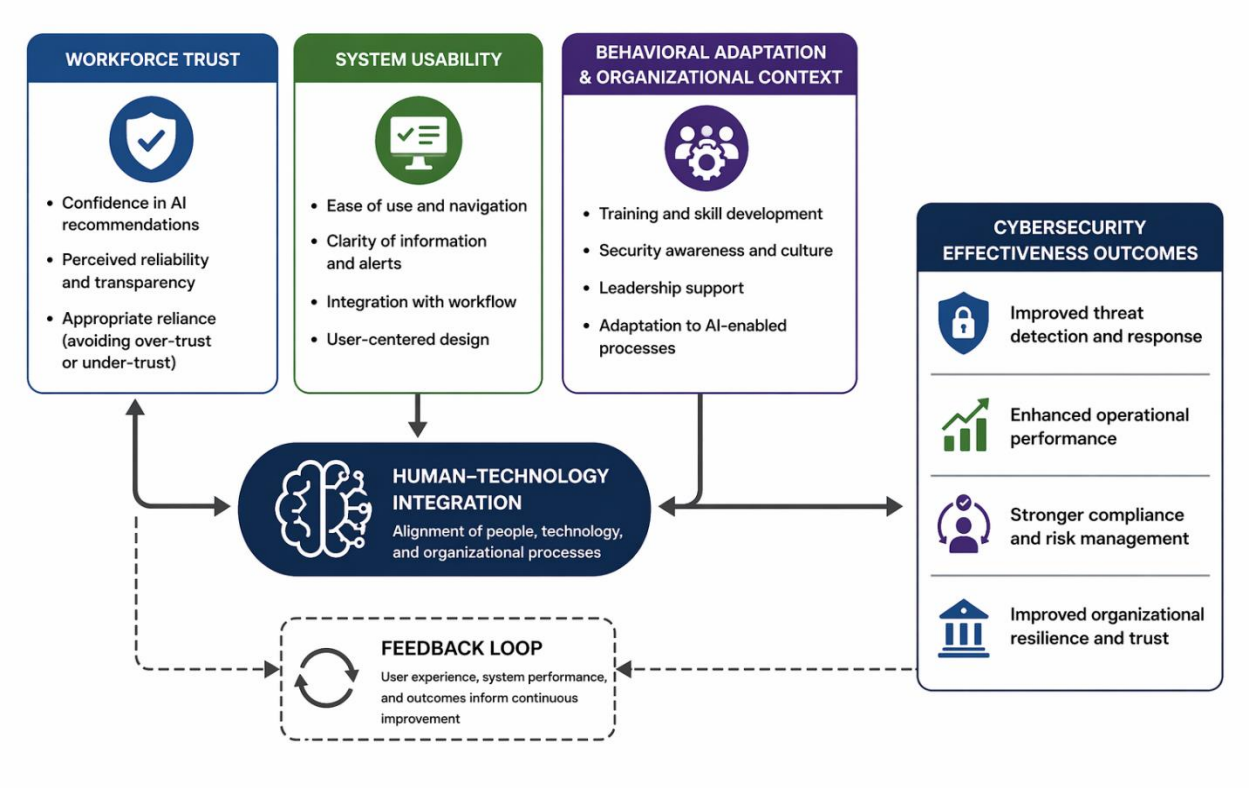
The Human–Technology Interaction Model is developed to conceptualize how human factors influence the effectiveness of AI-augmented cybersecurity systems within healthcare organizations. As organizations integrate advanced technological capabilities into security operations, system effectiveness becomes increasingly dependent on how users interpret, trust, and interact with these tools. This introduces a socio-technical condition in which technological performance alone is insufficient; rather, outcomes are shaped by the alignment between human behavior, system usability, and organizational context. The model conceptualizes how these interacting elements influence cybersecurity effectiveness and governance outcomes. Figure 1 presents the interaction between human factors and technological systems in shaping cybersecurity outcomes.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Figure 1

Human–Technology Interaction Model



Note. Author created. The model illustrates how trust, usability, and organizational context interact to influence the effectiveness of AI-enabled cybersecurity systems.

As illustrated in Figure 1, the interaction between trust, usability, and organizational context shapes the extent to which AI-enabled cybersecurity systems are effectively integrated into operational environments, influencing both workforce behavior and overall governance effectiveness.

The Human–Technology Interaction Model may also serve as a conceptual framework for assessing organizational readiness and the effectiveness of cybersecurity integration. Workforce trust may be operationalized through user confidence and reliance measures, while usability may be evaluated through workflow integration, interpretability, and consistency in adoption. Organizational culture and governance effectiveness may be examined through training participation, policy compliance, behavioral adaptation, and the integration of executive oversight. These dimensions provide a foundation for future empirical evaluation and organizational assessment.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Key Components of the Model:

- Trust in technology
- System usability
- Workforce behavior
- Organizational culture
- Governance oversight

5.1 Conceptual Propositions

The Human–Technology Interaction Model posits that the interplay between technological capabilities and human-centered organizational conditions influences cybersecurity effectiveness in AI-augmented healthcare environments.

The model advances the following conceptual propositions:

P1: Higher levels of workforce trust in AI-enabled cybersecurity systems are associated with greater operational integration and system utilization.

P2: Increased system usability improves workforce adoption, compliance, and cybersecurity effectiveness.

P3: Organizational cultures that support cybersecurity awareness, behavioral adaptation, and governance alignment strengthen the operational effectiveness of AI-enabled cybersecurity technologies.

P4: Governance frameworks that integrate human factors into cybersecurity oversight improve organizational resilience and technology adoption outcomes.

These propositions provide a conceptual foundation for future empirical validation and cross-sector comparative analysis.

6. Analytical Discussion

The analysis indicates that the effectiveness of AI-augmented cybersecurity systems is shaped not only by technical capability but also by the interaction between human factors and organizational governance structures. Prior research demonstrates that misalignment between technological systems and user behavior can reduce system effectiveness and introduce operational risk (Whitman & Mattord, 2017; Cuganesan et al., 2018). Additionally, governance literature emphasizes that effective cybersecurity outcomes depend on integrating human, technical, and organizational elements into a cohesive framework, particularly in complex environments such as healthcare (Nicho, 2018; Carayon, 2006).

Vol. 11, No. 03; 2026

ISSN: 2456-3676

6.1 Workforce Trust and System Effectiveness

Workforce trust significantly influences how AI-enabled cybersecurity systems are interpreted, integrated, and operationalized within healthcare environments. Trust affects whether users rely upon system outputs, incorporate automated recommendations into decision-making processes, and maintain confidence in cybersecurity operations during routine and high-pressure conditions. However, effective cybersecurity performance depends not merely on the presence of trust, but on the organization's ability to calibrate trust appropriately in relation to system capability, interpretability, and operational context.

Excessive trust in AI-enabled cybersecurity technologies may contribute to automation complacency, reduced independent situational assessment, and over-reliance on algorithmic recommendations. Under such conditions, workforce personnel may defer too heavily to automated outputs, thereby diminishing critical evaluation of cybersecurity alerts, threat indicators, and operational anomalies. Conversely, insufficient trust in AI-enabled systems may lead to alert disregard, inconsistent system utilization, operational workarounds, and fragmented cybersecurity practices, thereby reducing organizational resilience.

Trust relationships may become increasingly complex in AI-enabled environments, where the workforce's understanding of algorithmic decision-making remains limited. When cybersecurity systems operate as opaque or poorly interpretable "black-box" technologies, users may struggle to assess system reliability, validate automated outputs, or understand how cybersecurity decisions are generated. This interpretability gap may weaken workforce confidence, reduce operational integration, and complicate executive oversight of AI-enabled cybersecurity functions.

Consequently, organizations must approach workforce trust as an active governance and organizational management responsibility rather than as a passive byproduct of technological implementation. Effective trust calibration requires continuous workforce engagement, transparent communication regarding system capabilities and limitations, usability-centered implementation strategies, and governance structures that preserve human oversight and operational accountability. In healthcare settings, where cybersecurity incidents may directly affect patient safety and operational continuity, maintaining balanced trust relationships between workforce personnel and AI-enabled cybersecurity systems remains essential for sustaining organizational resilience and governance effectiveness.

6.2 Usability and Operational Integration

Usability significantly influences whether AI-enabled cybersecurity systems are effectively integrated into organizational workflows and operational decision-making processes. Although advanced cybersecurity technologies may provide sophisticated threat detection and automation capabilities, systems that are difficult to interpret, operationally disruptive, or poorly aligned with workforce routines may experience inconsistent adoption and reduced effectiveness. In

Vol. 11, No. 03; 2026

ISSN: 2456-3676

healthcare environments, where personnel frequently operate under time-sensitive and cognitively demanding conditions, usability limitations may directly affect cybersecurity compliance, workforce engagement, and operational resilience (Whitman & Mattord, 2017; Carayon, 2006).

AI-enabled cybersecurity systems that fail to align with operational workflows may unintentionally increase cognitive burden, disrupt clinical and administrative processes, and contribute to alert fatigue among workforce personnel. Under such conditions, users may struggle to distinguish between critical and non-critical alerts, reducing responsiveness to legitimate cybersecurity threats and encouraging desensitization to system notifications. Excessive operational complexity may also contribute to workflow avoidance behaviors, inconsistent system utilization, and the development of informal workarounds that weaken cybersecurity effectiveness and organizational oversight (Aldawood & Skinner, 2020; Almuhammadi & Alsaleh, 2021).

System interpretability further influences usability and operational integration. When cybersecurity tools provide outputs that are difficult to understand or insufficiently transparent, workforce personnel may struggle to assess system reliability, validate recommendations, or incorporate automated outputs into operational decision-making. These interpretability challenges may become particularly significant in AI-enabled environments where algorithmic processes operate with limited visibility into how conclusions, alerts, or risk assessments are generated. Consequently, operational integration depends not only on technological performance but also on the organization's ability to ensure that cybersecurity systems remain understandable, accessible, and functionally aligned with workforce responsibilities and organizational processes (Sarker, 2021; Butavicius et al., 2020).

From a governance perspective, usability should therefore be viewed not solely as a technical design consideration but as an organizational resilience and oversight factor that directly influences workforce behavior, operational consistency, and cybersecurity effectiveness. Effective governance requires organizations to incorporate usability-centered implementation strategies, workforce feedback mechanisms, adaptive training processes, and continuous evaluation of how cybersecurity technologies interact with operational workflows. Within healthcare systems, where cybersecurity disruptions may affect patient care, regulatory compliance, and organizational continuity, maintaining strong alignment between usability, workforce interaction, and governance oversight remains essential for sustainable cybersecurity performance (Nicho, 2018; Whitman & Mattord, 2017).

6.3 Behavioral Adaptation and Organizational Culture

Organizational culture shapes how employees respond to cybersecurity systems. Cuganesan et al. (2018) demonstrated that management influence and workplace norms play a key role in shaping security behavior.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

6.4 Governance Implications

Effective governance of AI-augmented cybersecurity systems requires organizations to move beyond purely technical oversight models toward integrated human-centered governance frameworks. Although AI-enabled cybersecurity technologies may improve operational efficiency, threat detection, and response capabilities, their effectiveness remains closely tied to workforce interaction, organizational culture, and behavioral adaptation processes (Carayon, 2006; Nicho, 2018).

Executive leadership must ensure that governance structures address not only technological implementation but also workforce trust calibration, usability integration, behavioral adaptation, and organizational readiness. Over-reliance on automated systems without sufficient workforce understanding may contribute to automation complacency, reduced situational awareness, and diminished independent judgment in cybersecurity. Conversely, insufficient trust in AI-enabled systems may lead to alert disregard, inconsistent system utilization, and fragmented operational practices (Butavicius et al., 2020; Sarker, 2021).

Governance mechanisms should therefore incorporate continuous workforce engagement, assessment of training effectiveness, integration of behavioral feedback, and organizational monitoring processes to evaluate how AI-enabled cybersecurity systems influence operational decision-making and cybersecurity culture. Human-centered governance structures should also establish clear accountability for AI oversight, workforce adaptation, and system interpretability to ensure that cybersecurity technologies remain aligned with organizational objectives and operational realities (Cuganesan et al., 2018; Aldawood & Skinner, 2020).

In healthcare environments, where cybersecurity events may directly affect patient safety, operational continuity, and regulatory compliance, governance effectiveness depends upon the organization's ability to integrate human, technical, and organizational dimensions into a cohesive cybersecurity strategy. Consequently, AI-enabled cybersecurity governance should be viewed not solely as a technological management function but as a socio-technical governance responsibility requiring continuous organizational adaptation, executive oversight, and workforce-centered resilience planning (Whitman & Mattord, 2017; Mbonihankuye et al., 2019; Kruse et al., 2017).

7. Practical Implications

Healthcare organizations should:

- Incorporate human factors into cybersecurity strategy
- Design systems with usability and clarity
- Provide training to build trust and competence
- Align governance frameworks with workforce behaviour

Vol. 11, No. 03; 2026

ISSN: 2456-3676

8. Limitations

This study is conceptual and grounded in case-informed analysis, which may limit generalizability across diverse healthcare settings. Additionally, the absence of empirical validation constrains the ability to assess the relationships proposed in the conceptual model quantitatively. Future empirical research is necessary to test and refine the model across organizational contexts and operational environments.

9. Future Research

Future research should empirically evaluate the Human–Technology Interaction Model across healthcare and other critical infrastructure sectors to examine how workforce trust, usability, behavioral adaptation, and governance oversight influence cybersecurity effectiveness in AI-enabled operational environments. Quantitative and mixed-methods studies examining relationships between workforce trust calibration, system interpretability, training effectiveness, organizational culture, and cybersecurity performance would help validate the socio-technical relationships proposed in this study.

Additional research should examine:

- Cross-sector comparisons of AI-enabled cybersecurity adoption and workforce adaptation
- Longitudinal analysis of organizational behavioral adaptation to AI-integrated cybersecurity systems
- The influence of explainable AI and system interpretability on workforce trust and operational decision-making
- Governance maturity models for human-centered AI cybersecurity oversight
- The relationship between organizational culture, cybersecurity awareness, and AI-system utilization
- Behavioral resilience frameworks for AI-enabled cybersecurity environments
- The impact of automation fatigue, cognitive overload, and alert saturation on cybersecurity effectiveness
- Executive governance strategies for balancing AI automation with human oversight and accountability

Future empirical investigations may also explore how healthcare organizations operationalize workforce trust calibration and behavioral governance monitoring within increasingly automated cybersecurity environments. As AI-enabled systems continue to evolve, understanding how organizations integrate human behavior, technological systems, and governance structures will remain essential for developing sustainable and resilience-oriented cybersecurity strategies.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

10. Conclusion

Human factors play a critical role in determining the effectiveness of AI-augmented cybersecurity systems within healthcare organizations. Although artificial intelligence technologies may improve threat detection, monitoring efficiency, and operational scalability, technical capability alone is insufficient to ensure sustainable cybersecurity outcomes. Rather, cybersecurity effectiveness depends upon how these technologies are interpreted, trusted, integrated, and operationalized within complex organizational environments.

The findings of this study demonstrate that workforce trust, usability, behavioral adaptation, organizational culture, and governance oversight collectively shape the operational performance of AI-enabled cybersecurity systems. Misalignment between technological systems and human interaction may contribute to automation complacency, alert fatigue, inconsistent adoption, and reduced organizational resilience. Consequently, cybersecurity governance must extend beyond technical implementation to incorporate human-centered organizational strategies that support workforce engagement, adaptive learning, and socio-technical integration.

The Human–Technology Interaction Model provides a conceptual foundation for understanding how organizational and behavioral dynamics influence cybersecurity effectiveness in AI-enabled healthcare environments. By integrating human factors into cybersecurity governance analysis, this study advances the broader understanding of cybersecurity as a socio-technical and organizational governance challenge rather than solely a technological problem.

Ultimately, successful AI-enabled cybersecurity governance requires organizations to balance technological innovation with workforce readiness, organizational adaptability, and executive oversight. Healthcare organizations must ensure that AI systems enhance operational resilience without weakening human judgment, accountability structures, or institutional governance capacity. Sustainable cybersecurity effectiveness, therefore, depends not only on intelligent technologies but also on the organization's ability to integrate human behavior, governance structures, and technological capability into a cohesive resilience-oriented cybersecurity strategy.

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.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

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 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

Vol. 11, No. 03; 2026

ISSN: 2456-3676

publication. The views expressed in this manuscript are those of the authors and do not necessarily represent the official positions of affiliated organizations.

References

Aldawood, H., & Skinner, G. (2020). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 12(5), 73.

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.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342–353.

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., & Pattinson, M. (2020). When believing in technology leads to poor cybersecurity: Development of a trust-in-technical-controls scale. *Computers & Security, 98*, Article 102020.

Carayon, P. (2006). Human factors of complex sociotechnical systems. *Applied Ergonomics, 37*(4), 525–535.

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology, 37*(1), 50–65.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1–10.

Mbonihankuye, S., Nkunzimana, A., & Ndagijimana, A. (2019). Healthcare data security technology: HIPAA compliance. Wireless Communications and Mobile Computing, 2019, Article 1927495.

National Institute of Standards and Technology. (2020). Cybersecurity supply chain risk management practices for systems and organizations (SP 800-161 Rev. 1). https://doi.org/10.6028/NIST.SP.800-161r1

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.

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