International Journal of Advanced Engineering and Management Research

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Integrating Technology, Human Factors, and Governance: A Socio-technical Framework for AI-enabled Cybersecurity 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.2026.11306 URL: http://dx.doi.org/10.51505/ijaemr.2026.11306

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

Abstract
This article develops a socio-technical framework for understanding the integration of artificial intelligence, human factors, and governance structures in healthcare cybersecurity environments. While prior research has examined technical capability, workforce interaction, and governance structures independently, limited work has synthesized these dimensions into a unified analytical framework. This study adopts a conceptual and integrative approach, informed by evidence from organizational cases, to examine how technological performance, human behavior, and governance oversight interact to influence cybersecurity effectiveness. The findings demonstrate that misalignment across these domains can reduce system effectiveness, while integrated alignment enhances organizational resilience and decision-making. The study introduces a socio-technical cybersecurity integration model and provides implications for healthcare leaders seeking to implement AI-enabled cybersecurity systems within complex organizational environments.

Keywords: socio-technical systems; cybersecurity governance; AI integration; human factors; healthcare cybersecurity; organizational resilience

1. Introduction

1.1 Background of the Problem

Healthcare organizations are increasingly integrating artificial intelligence (AI) and automated cybersecurity tools to address growing cyber threats and operational complexity. These technologies offer improved detection, efficiency, and scalability. However, cybersecurity effectiveness depends not only on technological capability but also on how these systems are integrated into organizational structures and human workflows.

Prior research has typically examined cybersecurity through isolated lenses—focusing either on technical performance, governance structures, or human behavior. This fragmented approach limits understanding of how these elements interact in real-world environments.

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 advancements in AI-enabled cybersecurity systems, organizations continue to face gaps in effectiveness due to misalignments among technology, human interaction, and governance structures. In healthcare settings, where operational complexity and regulatory requirements are high, failure to integrate these domains can lead to reduced visibility, inconsistent system use, and weakened oversight.

1.3 Purpose of the Article

The purpose of this article is to develop a socio-technical framework that integrates technological capability, human factors, and governance structures to explain cybersecurity effectiveness in healthcare organizations.

1.4 Research Questions

RQ1: How do technological, human, and governance factors interact to influence cybersecurity effectiveness?

RQ2: What risks emerge from misalignment across these domains?

RQ3: How can organizations achieve integrated socio-technical cybersecurity governance?

1.5 Contribution to the Literature

This article contributes by:

- Integrating three traditionally separate research domains
- Advancing socio-technical cybersecurity theory
- Providing a unified framework for AI-enabled cybersecurity governance

1.6 Series Integration and Positioning

This study builds on prior analyses of outsourced cybersecurity governance (Article 1) and workforce interactions with AI-enabled systems (Article 2) by offering an integrated socio-technical perspective. Whereas earlier articles examined governance structures and human factors independently, this study synthesizes these dimensions with technological capability to develop a comprehensive framework for cybersecurity effectiveness. This integrative approach establishes the foundation for subsequent analyses of regulatory alignment, executive decision-making, and organizational risk management within the broader research series.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

2. Literature Review

2.1 Technological Capability in Cybersecurity

Advances in AI and automation have significantly enhanced cybersecurity detection and response capabilities. However, technical performance alone does not guarantee organizational effectiveness. Whitman and Mattord (2017) emphasized that technical controls must be integrated with management and operational processes to achieve effective security outcomes.

Recent research further demonstrates that AI-enabled cybersecurity systems require integration between technological capability, organizational awareness, and workforce adaptability to achieve sustainable operational effectiveness (Sarker, 2021; Aldawood & Skinner, 2020).

2.2 Human Factors and Behavioral Interaction

Human interaction with cybersecurity systems plays a critical role in determining effectiveness. Trust, usability, and behavioral adaptation influence how systems are used and interpreted. Butavicius et al. (2020) demonstrated that user trust in technological controls affects reliance and decision-making, while Cuganesan et al. (2018) highlighted the influence of organizational culture and management on security behavior.

Contemporary research also emphasizes that cybersecurity behavior is strongly influenced by organizational culture, user-centered system design, and workforce education initiatives (Almuhammadi & Alsaleh, 2021).

2.3 Governance and Organizational Oversight

Cybersecurity governance provides the structure that coordinates technology and human interaction. Nicho (2018) emphasized that governance requires clear processes, accountability, and oversight. Schinagl and Shahim (2020) further argued that cybersecurity governance must be elevated to the level of organizational leadership.

2.4 Socio-Technical Systems Theory

Socio-technical systems theory provides a framework for understanding the interaction between technology, people, and organizational structures. Carayon (2006) emphasized that system effectiveness depends on alignment across these domains, particularly in complex environments such as healthcare.

2.5 Healthcare Organizational Context

Healthcare organizations face unique challenges due to regulatory requirements, distributed operations, and rapid technological change. Case evidence indicates that reliance on outsourced services, combined with limited internal staffing, can lead to governance fragmentation and operational misalignment.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Prior research has highlighted that healthcare organizations often face resource constraints and complex regulatory demands that complicate cybersecurity implementation (Kruse et al., 2017).

2.6 Literature Gap

Existing research has not sufficiently integrated technological, human, and governance dimensions into a unified framework. This gap limits organizations' ability to design and implement effective cybersecurity systems.

3. Theoretical Framework

This study integrates:

- Socio-Technical Systems Theory (Carayon, 2006)
- Cybersecurity Governance Frameworks (Nicho, 2018; Schinagl & Shahim, 2020)
- Organizational Behavior Theory

These frameworks support a holistic understanding of cybersecurity as an integrated system rather than isolated components.

4. Methodological Orientation

This study employs a qualitative conceptual integration approach informed by cybersecurity governance literature, human factors research, socio-technical systems theory, and case-informed evidence derived from healthcare cybersecurity environments (Carayon, 2006; Nicho, 2018; Schinagl & Shahim, 2020). The analytical process incorporates thematic synthesis techniques commonly associated with conceptual organizational and governance research to identify recurring patterns related to technological integration, workforce interaction, governance alignment, and cybersecurity effectiveness (Cuganesan et al., 2018; Whitman & Mattord, 2017). Rather than evaluating cybersecurity solely from a technical perspective, the study examines how technological capabilities, human interactions, and governance oversight collectively shape cybersecurity performance within complex healthcare organizations.

The conceptual analysis was guided by socio-technical systems theory, organizational behavior theory, and cybersecurity governance frameworks (Carayon, 2006; Nicho, 2018). These frameworks were used to examine how technological capabilities, human interactions, and governance structures collectively influence cybersecurity outcomes in AI-enabled healthcare environments. Prior research has emphasized that cybersecurity effectiveness depends on the alignment of organizational processes, workforce behavior, leadership oversight, and technical systems rather than isolated technological performance alone (Butavicius et al., 2020; Schinagl & Shahim, 2020).

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Case-informed observations were analytically evaluated through iterative thematic comparison to identify recurring socio-technical conditions affecting organizational cybersecurity implementation, governance coordination, and operational effectiveness (Cuganesan et al., 2018; Almuhammadi & Alsaleh, 2021). Analytical interpretation identified recurring patterns associated with governance fragmentation, workforce adaptation challenges, technological misalignment, and operational dependency conditions that may weaken cybersecurity resilience in healthcare organizations. These recurring themes informed the development of the Socio-Technical Cybersecurity Integration Model, which conceptualizes how alignment across technological, human, and governance domains shapes cybersecurity performance, organizational adaptability, and resilience capacity (Carayon, 2006; Whitman & Mattord, 2017).

Although the study does not seek statistical generalizability, the conceptual integration approach provides a structured analytical framework for understanding the effectiveness of cybersecurity in AI-enabled healthcare environments. By synthesizing technological, organizational, and behavioral dimensions into a unified socio-technical framework, the study advances cybersecurity governance scholarship beyond isolated technical or operational interpretations and toward a more integrated understanding of organizational cybersecurity resilience (Nicho, 2018; Schinagl & Shahim, 2020).

5. Conceptual Model

The Socio-Technical Cybersecurity Integration Model is developed to conceptualize how technological capability, human factors, and governance structures interact to influence cybersecurity effectiveness in healthcare organizations. As organizations increasingly deploy AI-enabled cybersecurity systems, effectiveness depends not only on technical performance but also on how these systems are integrated into organizational workflows, interpreted by users, and governed through oversight structures (Whitman & Mattord, 2017; Nicho, 2018). In complex healthcare environments, cybersecurity outcomes are shaped by continuous interaction among technological systems, workforce behavior, and organizational governance processes rather than by isolated technical controls alone (Carayon, 2006).

This model reflects a socio-technical perspective in which cybersecurity effectiveness emerges through alignment across three interdependent domains: technological capability, human behavior, and governance oversight. Technological capability includes AI-enabled detection systems, automation tools, data analytics, and operational monitoring processes. Human factors encompass workforce trust, usability perception, behavioral adaptation, learning processes, and cybersecurity culture. Governance structures provide oversight mechanisms involving accountability, strategic coordination, organizational policy, compliance management, and executive decision-making authority (Schinagl & Shahim, 2020; Cuganesan et al., 2018).

Misalignment across these domains may result in reduced system effectiveness, operational inefficiencies, fragmented oversight, inconsistent workforce adaptation, and increased organizational risk (Carayon, 2006; Butavicius et al., 2020). For example, technologically

Vol. 11, No. 03; 2026

ISSN: 2456-3676

advanced cybersecurity systems may become underutilized if workforce trust remains low or if governance structures fail to support integration into operational workflows. Similarly, strong governance structures may be weakened if technological systems generate excessive operational complexity or if users lack sufficient training and organizational support to effectively interpret cybersecurity outputs (Almuhammadi & Alsaleh, 2021).

Conversely, integrated alignment across technological capabilities, human interactions, and governance structures enhances cybersecurity effectiveness by strengthening organizational coordination, operational adaptability, decision-making consistency, and resilience (Whitman & Mattord, 2017; Nicho, 2018). Under integrated conditions, governance structures facilitate visibility and accountability, technological systems support operational responsiveness, and workforce adaptation reinforces organizational cybersecurity culture and coordinated decision-making.

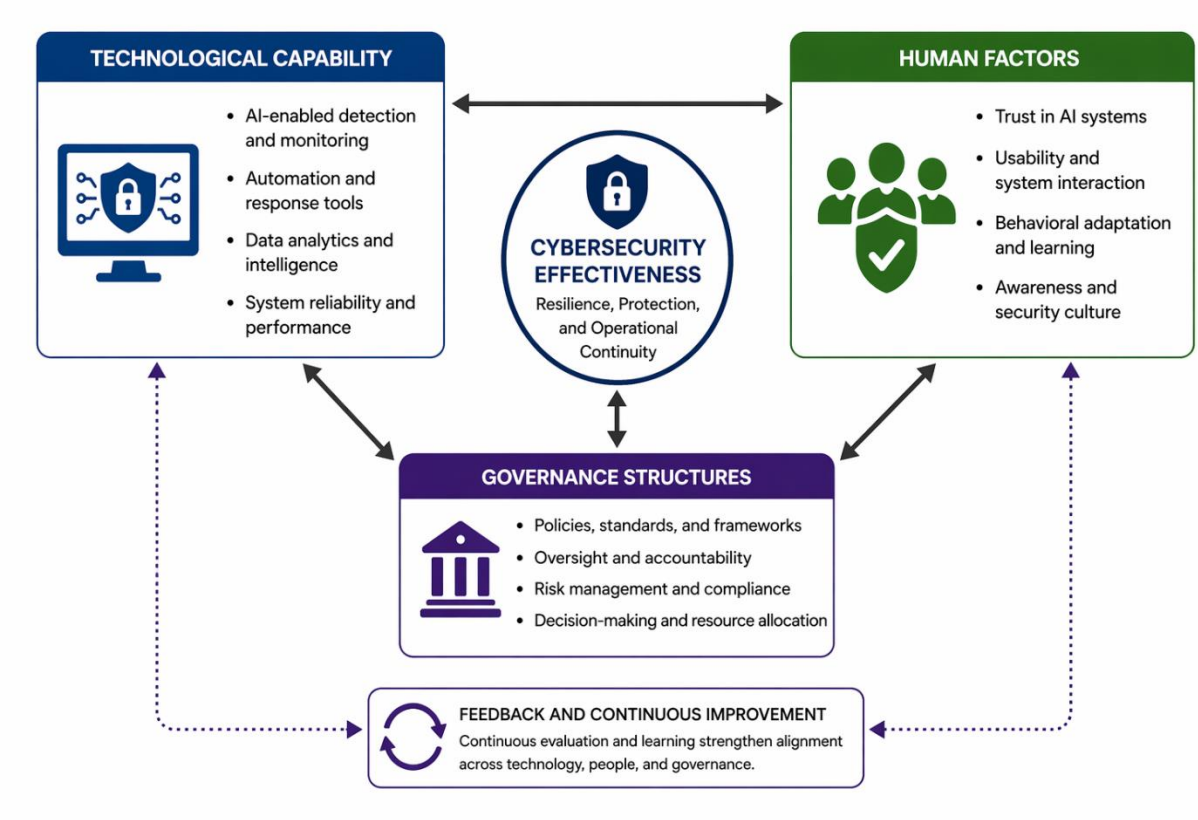
Figure 1 presents the Socio-Technical Cybersecurity Integration Model, which illustrates how cybersecurity effectiveness is shaped through dynamic interaction among technology, human behavior, and governance oversight within healthcare organizations.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Figure 1

Socio-Technical Cybersecurity Integration Model



Note. Author created. The model illustrates the interaction between technological capability, human factors, and governance structures in determining cybersecurity effectiveness.

As illustrated in Figure 1, cybersecurity effectiveness is maximized when technological systems, human interaction, and governance structures are aligned and integrated, enabling organizations to achieve coordinated, adaptive, and resilient cybersecurity operations.

Core Domains:

- Technological capability (AI systems, automation)
- Human factors (trust, usability, behavior)
- Governance structures (oversight, accountability, decision-making)

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Key Insight:

Cybersecurity effectiveness is maximized when technological systems, workforce interaction, and governance structures operate as an integrated socio-technical governance ecosystem rather than as isolated organizational components.

6. Analytical Discussion

6.1 Domain Interdependence

Cybersecurity effectiveness emerges from continuous interaction among technological capabilities, human behavior, and governance structures rather than from isolated technical performance alone (Carayon, 2006; Whitman & Mattord, 2017). In healthcare organizations, AI-enabled cybersecurity systems operate within complex socio-technical environments where technological outputs must be interpreted by users, coordinated through organizational workflows, and governed through oversight mechanisms. As a result, weaknesses within any single domain may reduce the effectiveness of the broader cybersecurity system and create cascading organizational vulnerabilities.

Technological capabilities enable organizations to implement advanced monitoring, detection, automation, and analytical functions to improve cybersecurity responsiveness and operational efficiency. However, technological systems alone cannot ensure organizational cybersecurity effectiveness if workforce trust, usability, and governance coordination remain underdeveloped (Butavicius et al., 2020; Sarker, 2021). AI-enabled systems require continuous interaction between human operators and governance structures to support accurate interpretation, operational responsiveness, and strategic oversight.

Human factors further influence how cybersecurity technologies are adopted, trusted, and operationalized within organizational environments. Workforce adaptation, system usability, organizational culture, and cybersecurity awareness shape whether employees effectively engage with AI-enabled cybersecurity systems or develop resistance, overreliance, or inconsistent usage behaviors (Almuhammadi & Alsaleh, 2021; Cuganesan et al., 2018). In healthcare settings, where operational pressures and rapid decision-making are common, ineffective human-system interactions can significantly reduce cybersecurity responsiveness and organizational coordination.

Governance structures provide the organizational mechanisms necessary to coordinate technological systems and workforce interaction through accountability, policy alignment, risk oversight, and executive decision-making processes (Nicho, 2018; Schinagl & Shahim, 2020). Governance effectiveness depends on maintaining visibility across operational processes while ensuring that technological implementation, workforce adaptation, and cybersecurity objectives remain strategically aligned. Consequently, cybersecurity resilience depends not only on

Vol. 11, No. 03; 2026

ISSN: 2456-3676

technical capability but also on the organization's ability to maintain coordinated socio-technical integration across all operational domains.

6.2 Misalignment Risks

Misalignment among technological systems, workforce behavior, and governance structures may introduce significant organizational cybersecurity risks. In socio-technical environments, technological capability alone cannot compensate for weak governance oversight, workforce distrust, or fragmented organizational coordination (Carayon, 2006). As organizations increasingly integrate AI-enabled cybersecurity technologies, cross-domain misalignment may lead to operational inefficiencies, inconsistent system utilization, reduced visibility, and weakened organizational resilience.

One significant risk involves underutilization or misuse of technological systems due to workforce adaptation challenges. AI-enabled cybersecurity systems often require users to interpret alerts, interact with automated recommendations, and incorporate technological outputs into operational workflows. When usability barriers, insufficient training, or low trust in automated systems exist, workforce engagement may decline, reducing the effectiveness of cybersecurity monitoring and incident response processes (Butavicius et al., 2020; Almuhammadi & Alsaleh, 2021). Conversely, excessive trust in automation may contribute to reduced independent verification, diminished situational awareness, and overreliance on technological interpretation.

Governance misalignment may also create fragmented oversight structures that limit organizational coordination and the effectiveness of decision-making. In healthcare settings, where cybersecurity governance responsibilities are often distributed among technical teams, administrators, compliance personnel, and executive leadership, insufficient integration among these groups may reduce clarity of accountability and operational responsiveness (Schinagl & Shahim, 2020; Nicho, 2018). Fragmented governance structures may further limit executive visibility into cybersecurity operations, particularly when AI-enabled systems generate complex operational outputs requiring cross-functional interpretation.

Case-informed observations also suggest that reliance on outsourced cybersecurity services, combined with limited internal cybersecurity capability, may exacerbate risks of socio-technical misalignment. Under such conditions, organizations may become increasingly dependent on external operational interpretation while simultaneously facing limitations in workforce adaptation and reduced visibility into governance. These dependency conditions may weaken institutional cybersecurity coordination, reduce organizational adaptability, and amplify systemic cybersecurity vulnerabilities during periods of operational disruption or rapid threat escalation.

Collectively, these findings suggest that socio-technical misalignment should be understood not merely as a technological implementation problem but as an organizational governance

Vol. 11, No. 03; 2026

ISSN: 2456-3676

challenge affecting cybersecurity resilience, workforce coordination, and strategic oversight capacity.

6.3 Integrated Governance Approach

Healthcare organizations must adopt integrated governance frameworks that align technological systems, workforce interaction, and organizational oversight within a coordinated socio-technical structure (Nicho, 2018; Schinagl & Shahim, 2020). Effective cybersecurity governance requires organizations to move beyond fragmented operational models toward integrated systems that continuously coordinate technological performance, human adaptation, and executive oversight processes.

An integrated governance approach requires establishing cross-functional coordination mechanisms to facilitate communication among cybersecurity personnel, executive leadership, compliance teams, operational managers, and workforce stakeholders. These mechanisms help ensure that technological implementation decisions remain aligned with organizational objectives, workforce capabilities, regulatory obligations, and enterprise risk management priorities (Whitman & Mattord, 2017). Integrated governance structures also strengthen organizational visibility into cybersecurity operations while reducing fragmentation across technical and administrative domains.

Continuous feedback and adaptation processes are essential components of socio-technical cybersecurity governance. Organizations must establish mechanisms to evaluate workforce interactions with AI-enabled systems, monitor governance effectiveness, assess operational usability, and identify emerging coordination challenges (Carayon, 2006; Cuganesan et al., 2018). These adaptive processes support organizational learning and allow governance structures to evolve alongside technological and operational changes.

Integrated governance additionally requires preserving internally retained cybersecurity capability sufficient to support independent organizational interpretation of technological outputs, vendor-generated reporting, and cybersecurity risk conditions. Excessive dependence on automation or external operational actors may reduce institutional cybersecurity literacy and weaken executive oversight capacity. Consequently, effective socio-technical governance depends on maintaining organizational visibility, strategic coordination, and internally coordinated cybersecurity expertise across AI-enabled operational environments.

6.4 Executive Implications

Executive leadership plays a critical role in ensuring alignment among technological capabilities, workforce interactions, and governance oversight in AI-enabled cybersecurity environments. Cybersecurity governance can no longer be treated solely as a technical operational function; rather, it must be integrated into enterprise-level strategic decision-making, organizational resilience planning, and risk governance processes (Schinagl & Shahim, 2020; Nicho, 2018).

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Leaders must ensure that cybersecurity governance structures provide sufficient visibility into technological operations, workforce adaptation, and organizational risk conditions. This includes establishing integrated reporting mechanisms, cross-functional oversight processes, and coordinated governance structures to support enterprise-wide cybersecurity decision-making (Whitman & Mattord, 2017). Executive oversight must additionally address the organizational implications of AI-enabled cybersecurity systems, including workforce trust calibration, usability integration, operational dependency risks, and accountability clarity.

Executive leadership must also preserve sufficient internal cybersecurity literacy to independently evaluate vendor-generated operational interpretations, automated system outputs, incident-escalation assessments, and strategic cybersecurity risks. As organizations increasingly integrate AI-enabled monitoring systems and outsourced cybersecurity functions, governance effectiveness depends on maintaining institutional capability to interpret operational conditions without excessive dependence on external technological or operational actors.

In healthcare settings, where cybersecurity failures can directly affect patient safety, operational continuity, regulatory compliance, and organizational resilience, executive leadership must ensure continuous alignment among technological systems, workforce interactions, and governance oversight. Effective socio-technical cybersecurity governance, therefore, requires not only advanced technical capability but also sustained executive engagement, coordinated organizational oversight, and adaptive governance structures capable of responding to evolving operational and cybersecurity conditions.

7. Practical Implications

Healthcare organizations implementing AI-enabled cybersecurity systems should adopt integrated socio-technical governance frameworks that coordinate technological capability, workforce interaction, and organizational oversight within a unified operational structure. Effective cybersecurity implementation depends not only on technological sophistication but also on the organization's ability to align governance processes, workforce adaptation, and operational decision-making across complex healthcare environments (Whitman & Mattord, 2017; Nicho, 2018).

Organizations should establish integrated cybersecurity governance structures that support cross-functional coordination among executive leadership, cybersecurity personnel, compliance teams, operational managers, and workforce stakeholders. These governance mechanisms strengthen organizational visibility into cybersecurity operations while reducing fragmentation across technical, administrative, and behavioral domains (Schinagl & Shahim, 2020). Integrated governance also improves accountability, clarity, consistency in decision-making, and organizational responsiveness during cybersecurity incidents and operational disruptions.

Effective implementation additionally requires alignment between technological systems and workforce capabilities. AI-enabled cybersecurity tools should be integrated into operational

Vol. 11, No. 03; 2026

ISSN: 2456-3676

workflows through user-centered design approaches, workforce training initiatives, continuous usability assessment, and adaptive learning processes (Almuhammadi & Alsaleh, 2021; Butavicius et al., 2020). Organizations that fail to support workforce adaptation adequately may experience reduced system utilization, inconsistent cybersecurity practices, and diminished operational effectiveness despite advanced technological capabilities.

Healthcare organizations should further implement continuous socio-technical feedback mechanisms that evaluate technological performance, workforce interaction, governance effectiveness, and operational coordination over time. These mechanisms may include integrated reporting systems, cross-functional governance reviews, workforce adaptation assessments, incident-response evaluations, and executive oversight reporting cycles (Carayon, 2006; Cuganesan et al., 2018). Continuous evaluation processes strengthen organizational learning while enabling governance structures to adapt alongside evolving cybersecurity conditions and technological developments.

Finally, organizations should maintain sufficient internal cybersecurity capability to preserve institutional visibility, strategic oversight, and independent operational interpretation within AI-enabled environments. Although technological systems and outsourced cybersecurity services may improve operational scalability, effective cybersecurity governance ultimately depends on the organization's ability to maintain coordinated socio-technical alignment, organizational adaptability, and resilience-oriented oversight structures across all cybersecurity domains.

8. Limitations

This study is conceptual and based on case-informed organizational analysis rather than direct empirical measurement, which may limit the generalizability of the findings across all healthcare environments and critical infrastructure sectors. The Socio-Technical Cybersecurity Integration Model reflects recurring socio-technical patterns derived from healthcare cybersecurity environments and may not fully capture variations associated with organizational size, cybersecurity maturity, workforce composition, technological infrastructure, or differing governance structures.

Additionally, the study emphasizes conceptual integration and governance interpretation rather than quantitative evaluation of cybersecurity performance outcomes. Although the analytical framework synthesizes technological, human, and governance dimensions into a unified socio-technical model, future empirical research is necessary to evaluate the strength, consistency, and operational applicability of the relationships proposed in this study.

The case-informed analytical approach may also reflect contextual conditions in healthcare cybersecurity environments characterized by operational complexity, distributed infrastructure, regulatory requirements, and increasing reliance on AI-enabled systems and outsourced cybersecurity services. Consequently, the framework may require adaptation when applied to

Vol. 11, No. 03; 2026

ISSN: 2456-3676

organizations operating in sectors with differing governance structures, operational demands, or technological integration models.

Despite these limitations, the study provides a structured socio-technical framework for advancing cybersecurity governance scholarship beyond isolated technological or operational interpretations. By integrating technological capabilities, workforce interactions, and governance oversight into a unified analytical framework, the study contributes to a broader understanding of cybersecurity effectiveness as an organizational and resilience-oriented governance challenge.

9. Future Research

Future studies should:

- Empirically test the integration model
- Examine cross-sector applications
- Analyze long-term implementation outcomes

Future research should also examine how socio-technical cybersecurity governance models operate across interconnected critical infrastructure sectors characterized by distributed operational architectures, regulatory fragmentation, and increasing reliance on AI-enabled cybersecurity systems.

10. Conclusion

Cybersecurity effectiveness in healthcare organizations depends on far more than technological capability alone. As organizations increasingly integrate AI-enabled cybersecurity systems into complex operational environments, cybersecurity outcomes are shaped through continuous interaction among technological systems, workforce behavior, and governance oversight structures. A socio-technical approach, therefore, provides a more comprehensive framework for understanding cybersecurity effectiveness than isolated technical or operational interpretations (Carayon, 2006; Whitman & Mattord, 2017).

The findings of this study demonstrate that misalignment among technological capabilities, human interactions, and governance coordination may reduce organizational visibility, weaken workforce adaptation, fragment oversight processes, and diminish cybersecurity resilience. Conversely, integrated alignment across these domains strengthens organizational coordination, operational adaptability, executive oversight, and resilience-oriented cybersecurity governance (Nicho, 2018; Schinagl & Shahim, 2020). Effective cybersecurity governance, therefore, depends not only on advanced technological implementation but also on the organization's ability to coordinate socio-technical interaction across all operational levels.

The Socio-Technical Cybersecurity Integration Model introduced in this study provides a conceptual framework for understanding how technological systems, workforce dynamics, and

Vol. 11, No. 03; 2026

ISSN: 2456-3676

governance structures collectively shape cybersecurity performance within healthcare environments. By conceptualizing cybersecurity as an integrated socio-technical governance condition rather than solely a technical function, this study advances a broader understanding of cybersecurity as an organizational, behavioral, and resilience-oriented challenge.

The study further demonstrates that executive leadership plays a central role in sustaining socio-technical alignment in cybersecurity. Organizations must preserve governance visibility, internally retain cybersecurity capability, workforce adaptability, and coordinated oversight structures capable of supporting strategic cybersecurity decision-making within AI-enabled operational environments. As healthcare organizations increasingly rely on automation, AI integration, and distributed cybersecurity architectures, governance effectiveness will depend on maintaining organizational control over strategic risk interpretation, operational coordination, and resilience management despite increasing technological complexity.

Ultimately, cybersecurity resilience in healthcare organizations depends on the continuous integration of technological capability, human factors, and governance oversight within adaptive socio-technical systems. Organizations that successfully align these domains will be better positioned to sustain cybersecurity effectiveness, strengthen organizational resilience, and respond to evolving cyber threats within increasingly complex healthcare and critical infrastructure 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

Vol. 11, No. 03; 2026

ISSN: 2456-3676

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

References

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

Vol. 11, No. 03; 2026

ISSN: 2456-3676

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

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., & Pattinson, M. (2020). When believing in technology leads to poor cybersecurity. *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). Management influence on information security behavior. *Behaviour & Information Technology, 37*(1), 50–65.

Nicho, M. (2018). 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.

Schinagl, S., & Shahim, A. (2020). Digital security governance. *Information & Computer Security, 28*(2), 261–292.

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