International Journal of Advanced Engineering and Management Research

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Outsourcing Cybersecurity: Governance Risks of Managed Security Service Provider (MSSP) Dependence 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.2026.11304 URL: http://dx.doi.org/10.51505/ijaemr.2026.11304

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

Abstract
This study examines the governance risks associated with dependence on managed security service providers (MSSPs) in healthcare organizations. As healthcare systems expand and face increasing regulatory, operational, and cybersecurity complexity, many organizations outsource critical security functions to external vendors. Although this approach may provide operational efficiency and access to specialized expertise, it can also create governance fragmentation, weaken internal oversight, and reduce institutional visibility into cyber risk management. Using a conceptual governance analysis informed by organizational case evidence from a multi-state healthcare provider, this study explores how MSSP dependence influences decision authority, accountability, compliance management, and strategic cybersecurity resilience. The article introduces a conceptual governance model to illustrate the structural risks of cybersecurity outsourcing. It provides practical implications for healthcare leaders seeking to balance outsourced capability with internal governance responsibility.

Keywords: cybersecurity governance; MSSP; outsourcing risk; healthcare cybersecurity; vendor oversight; cyber risk management

1. Introduction

1.1 Background of the Problem

Healthcare organizations operate within increasingly complex environments characterized by regulatory demands, distributed infrastructure, and heightened cyber risk. Protecting sensitive health data and maintaining operational continuity requires both advanced technical capabilities and strong governance structures. However, many healthcare organizations face resource constraints that limit their ability to maintain comprehensive internal cybersecurity operations.

As a result, organizations frequently outsource cybersecurity functions to managed security service providers (MSSPs), which offer scalable services such as monitoring, incident response, and infrastructure management. While outsourcing provides operational advantages, it also introduces governance challenges related to accountability, oversight, and risk ownership.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

In the healthcare case environment informing this study, the organization's IT infrastructure was largely outsourced, with only a limited internal team responsible for vendor coordination, despite rapid multi-state expansion and increasing system complexity. This configuration reflects a broader governance concern in which operational control is externalized while accountability remains internal.

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 increased reliance on MSSPs, healthcare organizations continue to face governance failures that undermine the effectiveness of cybersecurity. Outsourcing critical functions may lead to fragmented decision-making, reduced visibility into security operations, and unclear accountability structures, creating a governance gap between execution and responsibility.

1.3 Purpose of the Article

The purpose of this article is to examine how MSSP dependence influences the effectiveness of cybersecurity governance in healthcare organizations, with an emphasis on accountability, oversight, and decision-making authority.

1.4 Research Questions

RQ1: How does MSSP dependence influence cybersecurity governance effectiveness?

RQ2: What governance risks emerge from outsourcing cybersecurity operations?

RQ3: What organizational implications arise from MSSP-driven cybersecurity models?

1.5 Contribution to the Literature

This article contributes to the cybersecurity governance literature by extending existing research on outsourcing and third-party cyber risk into the domain of organizational governance and executive oversight. While prior studies have examined cybersecurity outsourcing primarily from operational and technical perspectives, this study advances the literature by conceptualizing MSSP dependence as a governance condition that restructures accountability, visibility, and decision authority within healthcare organizations.

2. Literature Review

2.1 Cybersecurity Governance

Cybersecurity governance aligns security practices with organizational objectives, ensuring accountability, oversight, and strategic integration. Effective governance requires leadership

Vol. 11, No. 03; 2026

ISSN: 2456-3676

involvement, structured processes, and organizational alignment (Whitman & Mattord, 2017; Nicho, 2018).

Schinagl and Shahim (2020) emphasized that cybersecurity governance must extend beyond technical controls to encompass organizational oversight and leadership engagement. Additionally, Cuganesan et al. (2018) demonstrated that managerial influence and organizational norms significantly shape cybersecurity behavior and effectiveness.

2.2 Outsourcing and MSSP Dependence

Outsourcing cybersecurity functions provides access to specialized expertise but introduces dependency risks and governance challenges related to oversight, control, and accountability. In healthcare environments, reliance on MSSPs can reduce internal control and limit visibility into security operations, particularly when vendor activities are not fully integrated into organizational governance structures (Boyson, 2014; NIST, 2020). Research on cybersecurity supply chain risk emphasizes that third-party dependencies can create systemic vulnerabilities if governance mechanisms are insufficiently developed or enforced (National Institute of Standards and Technology [NIST], 2020). In healthcare settings, these risks are amplified due to regulatory requirements and the sensitivity of patient data, necessitating stronger integration between outsourced services and internal governance processes (Kruse et al., 2017).

2.3 Organizational Governance Theory

Organizational governance theory highlights the importance of clear authority, accountability, and oversight structures. Socio-technical systems perspectives further emphasize that effective security depends on alignment between technology, human actors, and organizational processes (Carayon, 2006).

2.4 Healthcare Cybersecurity Context

Healthcare organizations face unique governance challenges due to regulatory requirements and operational complexity. Mbonihankuye et al. (2019) noted that healthcare cybersecurity requires integrated governance and technical controls to maintain compliance and protect sensitive data.

2.5 Literature Gap

Although prior research addresses cybersecurity governance and outsourcing, limited attention has been given to MSSP dependence as a governance structure that affects accountability, visibility, and risk ownership in healthcare organizations. Additionally, limited research has examined how emerging technologies such as artificial intelligence-enabled monitoring systems and automated compliance platforms may influence governance dependency relationships between healthcare organizations and MSSPs.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

3. Theoretical and Conceptual Framework

This study integrates:

- Enterprise Risk Management (ERM)
- Organizational governance theory
- Socio-technical systems theory

These frameworks support the analysis of MSSP dependence as a governance condition influencing organizational risk oversight and decision-making.

4. Methodological Orientation

This study adopts a qualitative conceptual governance approach informed by cybersecurity governance scholarship, enterprise risk management theory, socio-technical systems analysis, and organizational evidence derived from a multi-state healthcare environment (Carayon, 2006; Nicho, 2018; Schinagl & Shahim, 2020). Rather than examining cybersecurity outsourcing solely as a technical or operational issue, the analysis examines how dependence on MSSPs restructures organizational accountability, visibility, and governance authority within complex healthcare systems (Whitman & Mattord, 2017; De Haes & Van Grembergen, 2009).

The analytical process incorporated interpretive thematic synthesis techniques commonly utilized in organizational governance and socio-technical research to evaluate patterns associated with outsourced operational control, executive oversight limitations, accountability diffusion, and institutional dependency structures (Carayon, 2006; Cuganesan et al., 2018). Enterprise Risk Management (ERM), organizational governance theory, and socio-technical systems theory collectively informed the analytical interpretation of governance relationships between internal leadership structures and external cybersecurity providers (De Haes & Van Grembergen, 2009; Nicho, 2018).

Analytical interpretation of the organizational environment identified persistent governance asymmetries between externally managed cybersecurity operations and internally retained accountability obligations. These conditions revealed structural tensions associated with reduced operational visibility, distributed decision authority, and reliance on external cybersecurity expertise (Boyson, 2014; NIST, 2020). The resulting analytical synthesis informed the development of the MSSP Governance Dependency Model, which conceptualizes how outsourcing arrangements may generate governance dependency conditions that influence cybersecurity resilience, oversight effectiveness, and executive risk management (Schinagl & Shahim, 2020; Whitman & Mattord, 2017).

Vol. 11, No. 03; 2026

ISSN: 2456-3676

5. Conceptual Governance Model

The MSSP Governance Dependency Model is developed to conceptualize the structural implications of outsourcing cybersecurity operations within healthcare organizations. As reliance on external service providers increases, operational cybersecurity functions—including monitoring, detection, and response—are transferred to MSSPs, while ultimate accountability for risk management, regulatory compliance, and organizational outcomes remains internal (Whitman & Mattord, 2017; Nicho, 2018). This structural configuration introduces a governance condition in which control and responsibility are distributed across organizational boundaries, creating challenges related to visibility, coordination, and decision-making authority (Schinagl & Shahim, 2020; Carayon, 2006). In healthcare environments, where cybersecurity is closely tied to regulatory compliance and patient safety, this separation may amplify governance complexity and risk exposure (Mbonihankuye et al., 2019). The model conceptualizes how the structural separation between operational control and accountability influences the effectiveness of cybersecurity governance and organizational risk oversight.

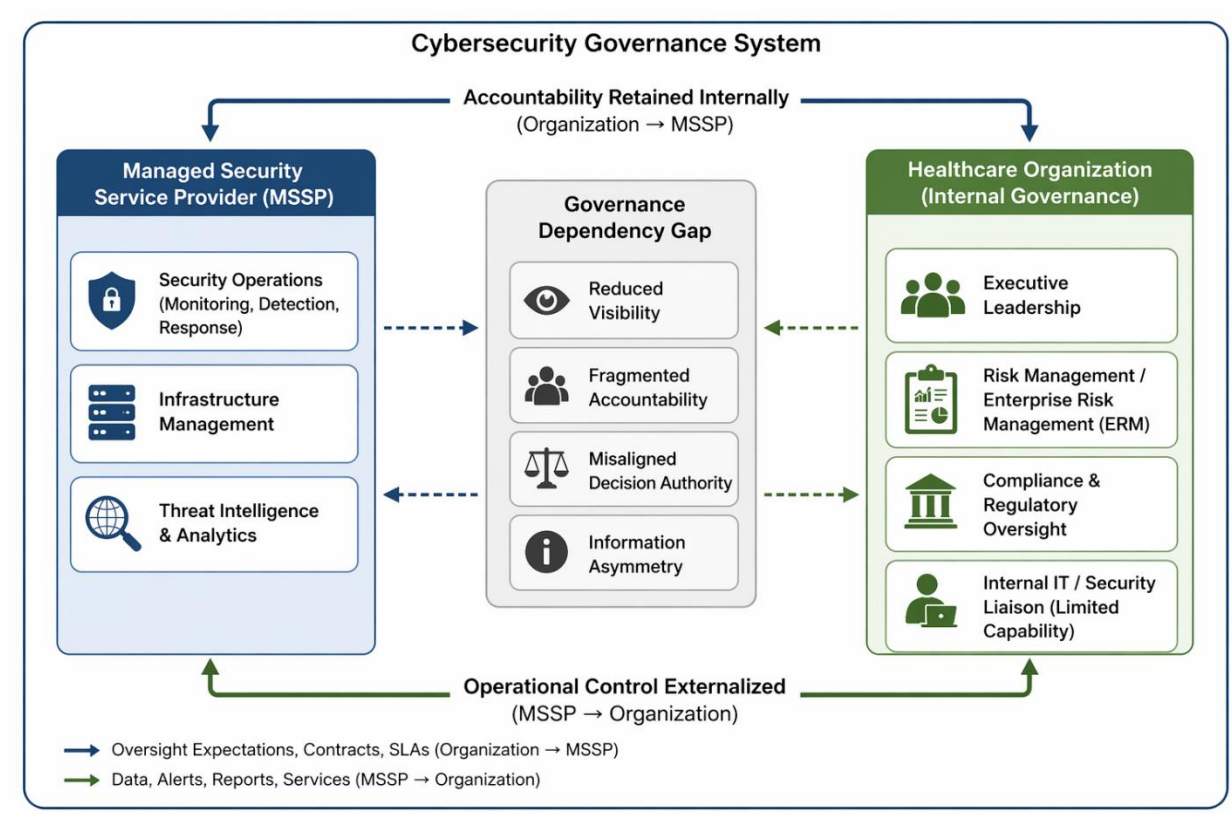
Figure 1 illustrates how MSSP reliance restructures cybersecurity governance by externalizing operational control while retaining internal accountability, creating a governance dependency gap that affects visibility, decision authority, and risk oversight.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Figure 1

MSSP Governance Dependency Model



Note. Author created. The model illustrates how outsourced cybersecurity operations shift operational control to external providers while organizational accountability remains internal, creating governance dependency.

As illustrated in Figure 1, MSSP dependence introduces a structural separation between operational control and governance accountability, requiring healthcare organizations to implement integrated oversight mechanisms that restore visibility, align decision authority, and mitigate governance dependency risk.

This governance dependency condition may become increasingly significant as healthcare organizations expand operational scale, integrate distributed infrastructures, and rely more heavily on outsourced cybersecurity services to manage organizational complexity. Under such conditions, executive leadership may become increasingly dependent on externally generated operational interpretations, potentially limiting independent organizational assessment of cybersecurity readiness, systemic vulnerabilities, and incident-escalation severity. Consequently, governance effectiveness depends not only on technical capability but also on the organization's

Vol. 11, No. 03; 2026

ISSN: 2456-3676

ability to preserve institutional visibility, strategic oversight, and internally coordinated risk governance across outsourced cybersecurity environments.

Core Components:

- Externalized operational control
- Reduced internal visibility
- Fragmented accountability
- Misaligned decision authority
- Governance dependency risk

6. Analytical Discussion

6.1 Structural Drivers of MSSP Dependence

Workforce shortages, cost efficiency, and rapid organizational expansion often drive MSSP reliance (Boyson, 2014; Kruse et al., 2017). In the case environment, limited internal staffing combined with extensive outsourcing created a governance imbalance in which operational cybersecurity dependence increasingly exceeded the capability of internally retained oversight, thereby amplifying organizational reliance on vendor-generated operational interpretation and external technical expertise (Whitman & Mattord, 2017; Schinagl & Shahim, 2020).

6.2 Governance Risks

Key governance risks associated with dependence on MSSPs include reduced organizational visibility into cybersecurity operations, fragmented accountability structures, over-reliance on external providers, and gradual erosion of internal cybersecurity capabilities. These findings align with research emphasizing the importance of integrated governance structures and sustained internal oversight in maintaining effective cybersecurity programs (Whitman & Mattord, 2017; De Haes & Van Grembergen, 2009). Additionally, cybersecurity supply chain risk literature highlights that excessive dependence on external providers may introduce systemic vulnerabilities extending beyond technical operations into strategic governance and enterprise risk domains (NIST, 2020; Boyson, 2014).

As healthcare organizations increasingly externalize operational cybersecurity functions, governance asymmetries may arise between organizations that retain accountability and MSSPs that exercise operational control. Although responsibility for regulatory compliance, enterprise risk management, and organizational resilience remains internal, operational visibility may increasingly depend on vendor-generated reporting, escalation practices, and interpretive frameworks (Schinagl & Shahim, 2020; De Haes & Van Grembergen, 2009). This condition may create information asymmetries that limit executive awareness of emerging threats, operational vulnerabilities, and systemic governance weaknesses (Boyson, 2014; Nicho, 2018).

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Over time, persistent reliance on MSSPs may also contribute to the erosion of institutional cybersecurity capabilities. As strategic expertise, operational familiarity, and technical decision-making become concentrated within external providers, healthcare organizations may experience reduced internal capacity to independently evaluate cybersecurity performance, validate vendor actions, or exercise informed governance oversight (Whitman & Mattord, 2017; Carayon, 2006). This dependency condition may weaken organizational resilience during major incidents, vendor disruptions, contractual conflicts, or rapid threat escalation scenarios (NIST, 2020; Boyson, 2014).

Furthermore, MSSP dependence may unintentionally shift portions of cybersecurity governance authority toward external operational actors. Although MSSPs are typically engaged to provide technical services, their influence over monitoring, detection, reporting, and incident interpretation may position them as de facto participants in organizational risk governance processes (Schinagl & Shahim, 2020; De Haes & Van Grembergen, 2009). Without integrated oversight structures, this diffusion of operational influence may complicate executive decision-making, undermine clarity of accountability, and reduce organizational control over cybersecurity strategy (Nicho, 2018; Whitman & Mattord, 2017).

To reduce information asymmetry between healthcare organizations and MSSPs, governance structures should incorporate both technical and administrative mechanisms for integration. These mechanisms may include real-time cybersecurity dashboard integration, shared incident-escalation protocols, mandatory joint incident-response exercises, continuous governance reporting cycles, and formal communication channels between executive leadership and MSSP operational teams (Carayon, 2006; Cuganesan et al., 2018). Such mechanisms help restore organizational visibility into outsourced cybersecurity operations while strengthening coordination, accountability, and executive oversight (De Haes & Van Grembergen, 2009; NIST, 2020).

Collectively, these governance conditions suggest that MSSP dependence should be evaluated not solely as an operational outsourcing arrangement but as a strategic challenge to organizational resilience requiring continuous executive oversight, integrated governance coordination, and sustained internal cybersecurity capability development.

6.3 Executive Implications

Leadership must ensure clear accountability structures, robust vendor oversight frameworks, and the integration of outsourced cybersecurity operations into internal governance systems. Effective governance requires not only technical oversight but also alignment between external service providers and organizational risk management processes (De Haes & Van Grembergen, 2009; NIST, 2020). Executive leadership must also preserve sufficient internal cybersecurity literacy and governance visibility to independently evaluate vendor-generated operational interpretations, incident-severity assessments, and strategic risk implications.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

7. Practical Implications

Healthcare organizations should implement integrated vendor governance frameworks that maintain executive oversight despite outsourced cybersecurity operations. Effective governance requires balancing external technical capability with internally retained accountability structures.

Recommended governance practices include:

- Establishing vendor governance committees responsible for MSSP oversight and performance evaluation
- Maintaining internal cybersecurity leadership roles with authority over enterprise risk decisions
- Defining decision rights that distinguish internally retained governance responsibilities from outsourced operational functions
- Implementing real-time reporting dashboards that provide organizational leadership with direct visibility into cybersecurity events and MSSP activities
- Conducting joint incident response exercises involving both internal leadership teams and MSSP personnel
- Developing hybrid cybersecurity governance models that combine internal strategic oversight with external operational support
- Aligning MSSP contracts with enterprise risk management objectives, regulatory requirements, and organizational accountability expectations

Examples of governance functions that should remain internal include:

- Enterprise risk acceptance decisions
- Regulatory compliance accountability
- Executive cybersecurity strategy
- Incident escalation authority
- Organizational policy development

Operational functions that may be outsourced include:

- Security monitoring
- Threat detection
- Vulnerability scanning
- Infrastructure support services
- Routine incident triage

8. Limitations

This study is conceptual and based on case-derived organizational evidence rather than direct empirical measurement, which may limit the generalizability of the findings across all healthcare

Vol. 11, No. 03; 2026

ISSN: 2456-3676

environments and critical infrastructure sectors. Additionally, the MSSP Governance Dependency Model reflects governance patterns derived from a specific multi-state healthcare operational context and may not fully capture variations across organizational size, cybersecurity maturity, regulatory environments, or differing outsourcing structures. Because the analysis emphasizes governance interpretation rather than quantitative measurement, future empirical validation is necessary to evaluate the strength and consistency of the governance relationships proposed in this study.

9. Future Research

Future research should empirically evaluate the MSSP Governance Dependency Model across healthcare and other critical infrastructure sectors. Quantitative studies examining relationships between internal cybersecurity staffing ratios, MSSP dependence levels, incident response performance, regulatory compliance outcomes, and organizational resilience metrics would help validate the governance relationships proposed in this study.
Additional research should examine:

- Cross-sector governance comparisons
- Hybrid governance effectiveness
- MSSP governance maturity models
- Executive cybersecurity oversight effectiveness
- The influence of artificial intelligence and automated compliance systems on outsourced cybersecurity governance structures

Future empirical studies may also evaluate whether increased automation and AI-enabled governance monitoring reduce or amplify information asymmetry and organizational dependency risks associated with cybersecurity outsourcing.

10. Conclusion

MSSP dependence introduces governance risks that extend far beyond technical outsourcing considerations. As healthcare organizations increasingly externalize cybersecurity operations, they may unintentionally create governance asymmetries in which operational control is distributed across organizational boundaries. At the same time, accountability for risk, compliance, and resilience remains internal. This structural separation may reduce visibility, diffuse decision authority, and weaken institutional cybersecurity capability over time.

The findings of this study demonstrate that effective cybersecurity governance cannot be achieved solely through outsourced technical expertise. Rather, organizational resilience depends on the integration of external cybersecurity services within internally coordinated governance frameworks that preserve executive oversight, clarity of accountability, and strategic risk ownership.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

The MSSP Governance Dependency Model provides a conceptual foundation for understanding how outsourced cybersecurity relationships influence the effectiveness of organizational governance in complex healthcare environments. By conceptualizing cybersecurity outsourcing as a governance condition rather than solely an operational arrangement, this study advances the broader understanding of cybersecurity as an integrated socio-technical and organizational challenge.

Ultimately, healthcare organizations must ensure that cybersecurity outsourcing enhances organizational capability without diminishing institutional governance authority. As critical infrastructure sectors increasingly integrate outsourced cybersecurity ecosystems, governance effectiveness will depend on organizations' ability to maintain institutional control over strategic risk interpretation, executive oversight, and resilience coordination despite distributed operational architectures. Cybersecurity operations may be outsourced, but accountability for organizational resilience, regulatory compliance, and enterprise risk governance remains an internal executive responsibility.

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.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

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

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

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.

De Haes, S., & Van Grembergen, W. (2009). *An exploratory study into IT governance implementations and its impact on business/IT alignment.* Information Systems Management, 26(2), 123–137.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

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.

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? *Information & Computer Security, 28*(2), 261–292.

Stallings, W., & Brown, L. (2017). *Computer security: Principles and practice* (4th ed.). Pearson.

Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational violations of externally governed privacy and security rules. *Journal of the Association for Information Systems, 17*(1), 39–76.

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