International Journal of Advanced Engineering and Management Research

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Governance Fragmentation and Cybersecurity Blind Spots in Critical Infrastructure Organizations

Dr. Robb Shawe (Lead Author)
Dr. Gilbert B. Mengnjo (Co-Author)

doi.org/10.51505/ijaemr.2026.1204 URL: http://dx.doi.org/10.51505/ijaemr.2026.1204

Received: Feb 21, 2026 Accepted: Mar 02, 2026 Online Published: Mar 09, 2026

Abstract

Cybersecurity failures in critical infrastructure organizations are frequently attributed to technical deficiencies, human error, or insufficient investment in security controls. While these factors contribute to risk, they often obscure a more profound and more persistent cause: fragmented governance structures that diffuse responsibility, weaken accountability, and create predictable cybersecurity blind spots. In large, complex organizations—particularly in healthcare and energy sectors—cybersecurity spans multiple functional domains, including information technology, operational technology, compliance, legal, procurement, and enterprise risk management. When governance authority and oversight are fragmented across these domains, no single entity retains visibility into system-level exposure. This qualitative, conceptual analysis examines governance fragmentation as a root cause of cybersecurity blind spots in critical infrastructure organizations. Drawing on governance and accountability theory, organizational design literature, and boundary-spanning concepts, the article explains how fragmented structures undermine oversight even in organizations that employ standardized assessments and maturity models. The study contributes a governance-centric explanation for persistent cyber risk and offers implications for redesigning accountability and oversight structures to reduce systemic exposure.

Keywords: Cybersecurity governance; organizational fragmentation; accountability; cybersecurity blind spots; critical infrastructure; healthcare; energy systems; enterprise risk management

1. Introduction

This article advances the argument that governance fragmentation within critical infrastructure organizations produces persistent cybersecurity blind spots, independent of the systemic origins of risk or the mechanisms used for board-level reporting and oversight. Cybersecurity has become a defining governance challenge for critical infrastructure organizations, including healthcare systems and energy providers that rely on digitally integrated environments to sustain operations (Cybersecurity and Infrastructure Security Agency [CISA], 2024; U.S. Department of Energy [DOE], 2022). As cyber threats grow in scale and sophistication, organizations have

Vol. 11, No. 02; 2026

ISSN: 2456-3676

invested heavily in technical controls, monitoring tools, and compliance programs intended to reduce exposure.

In this article, the term cybersecurity assessment outputs refers to the structured findings generated by standardized cybersecurity assessment instruments. Despite these investments, cybersecurity incidents continue to reveal significant blind spots—areas of unrecognized or underestimated risk that persist until disruption occurs (Boyens et al., 2022). These blind spots are often attributed to technical oversights or isolated human failures. However, such explanations overlook a more fundamental organizational condition:

structural accountability fragmentation.

In large organizations, cybersecurity responsibilities are distributed among technical teams, operational units, compliance offices, legal departments, procurement functions, and executive leadership (National Institute of Standards and Technology [NIST], 2024). This fragmentation creates predictable governance gaps in which risks fall between organizational boundaries. Prior doctoral research in healthcare supply chain cybersecurity and energy governance similarly demonstrates that cyber risk persists where accountability and oversight are structurally misaligned (Mengnjo, 2026; Shawe, 2026). Moreover, this article argues that governance fragmentation is a root cause of persistent cybersecurity blind spots in critical infrastructure organizations. It reframes these blind spots as governance failures rather than technical anomalies.

This manuscript is part of a larger research initiative that explores the interpretation of cybersecurity governance within critical infrastructure environments. The series examines the impact of cybersecurity assessments, maturity models, and governance frameworks on organizational learning, risk prioritization, and resilience in complex socio-technical systems. By integrating multidisciplinary academic analysis with practitioner-informed insights, the research aims to clarify how governance design, regulatory frameworks, and organizational accountability influence the effectiveness of cybersecurity risk management and operational resilience.

1.1 Methodological Orientation

This study adopts a qualitative governance analysis informed by organizational design theory, accountability scholarship, and the literature on cybersecurity governance. The approach is conceptual and analytical, examining how structural fragmentation in large, complex organizations produces cybersecurity blind spots independent of technical control adequacy.
The analysis integrates governance theory with sector-specific scholarship in healthcare and energy infrastructure to identify structural accountability gaps. Rather than presenting new empirical data, the article synthesizes theoretical perspectives and documented sector characteristics to explain how distributed authority, diffused responsibility, and weak escalation pathways generate persistent exposure.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

2. Background and Context

2.1 Governance fragmentation in complex organizations

Fragmented oversight structures are a well-documented feature of large, complex organizations. Organizational design literature shows that specialization and siloing improve local efficiency but degrade system-level coordination and accountability when responsibilities span multiple domains (Boyens et al., 2022).

In critical infrastructure organizations, fragmentation is intensified by regulatory layering, safety mandates, and the convergence of information technology (IT) and operational technology (OT), resulting in split authority over cyber risk governance (DOE, 2022).

2.2 Cybersecurity research emphasizing technical gaps

Much cybersecurity research emphasizes vulnerabilities, adversarial techniques, and control failures, often treating organizations as coherent actors (NIST, 2024). While technically valuable, this perspective obscures the governance conditions that allow risks to persist even when controls exist.

2.3 Fragmented accountability in infrastructure sectors

Evidence from the healthcare and energy sectors indicates that cybersecurity accountability is routinely fragmented across IT, OT, compliance, vendor management, and executive leadership, resulting in blind spots at organizational interfaces (CISA, 2024; Mengnjo, 2026; Shawe, 2026).

2.4 Gap in existing analysis

Despite recognition of organizational silos, limited scholarship treats cybersecurity blind spots as outcomes of governance fragmentation. A governance-centric explanation is therefore needed to explain why risks remain invisible to leadership until disruption occurs. This analysis forms part of a broader, multi-article research program examining the governance and interpretation of cybersecurity assessment outputs across critical infrastructure contexts (Shawe, 2026).

3. Problem Statement

It is not known how structurally fragmented governance arrangements contribute to persistent cybersecurity blind spots in critical infrastructure organizations.

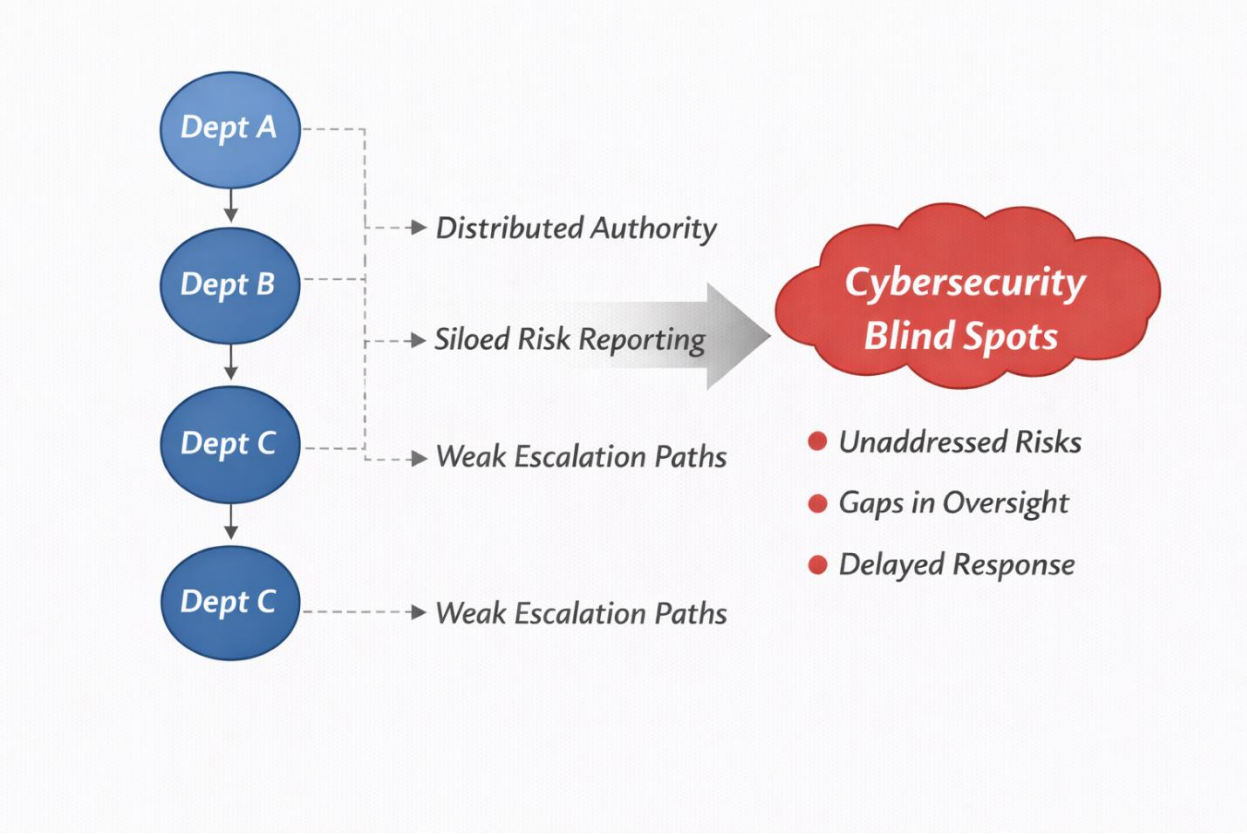
Fragmentation diffuses responsibility, weakens escalation pathways, and limits executive visibility into system-level cyber risk, increasing the likelihood of undetected exposure and delayed response (Boyens et al., 2022; NIST, 2024). To clarify the structural dynamics through which distributed authority and fragmented oversight produce cybersecurity blind spots in complex organizations, the governance-fragmentation model developed in this study is illustrated in Figure 1.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Figure 1

Governance Fragmentation and the Formation of Cybersecurity Blind Spots



Note. Author created. The figure depicts how distributed authority, siloed risk reporting, and weak escalation pathways diffuse accountability across organizational units, resulting in unaddressed risks, oversight gaps, and delayed response. The model is conceptual and supports the governance-fragmentation framework developed in this study.

The structural mechanism through which fragmented governance arrangements generate cybersecurity blind spots is illustrated in Figure 1.

4. Purpose of the Study

The purpose of this qualitative analysis is to examine how governance fragmentation creates cybersecurity blind spots within healthcare and energy infrastructure organizations, focusing on the distribution of accountability, oversight mechanisms, and executive visibility rather than on technical controls.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

5. Research Questions

RQ1: How is cybersecurity responsibility distributed across organizational units in critical infrastructure organizations?

RQ2: Where do governance gaps emerge between technical, operational, and executive functions?

RQ3: How do standardized cybersecurity assessments expose—but fail to resolve—governance blind spots?

6. Theoretical and Conceptual Framework

This analysis integrates three complementary perspectives.

Governance and accountability theory emphasizes the alignment of authority, responsibility, and oversight, highlighting that fragmented authority undermines effective risk governance (Boyens et al., 2022).

Organizational design and fragmentation theory explain how specialization and siloing degrade coordination and system-level accountability.

Boundary-spanning and coordination theory focuses on interfaces between organizational units, where cybersecurity blind spots frequently emerge due to incomplete information and diffused authority (Shawe, 2026).

Together, these lenses explain why cybersecurity blind spots persist even in organizations operating under **diffused governance arrangements**, despite the use of standardized assessments and maturity models (Mengnjo, 2026).

7. Significance of the Study

This study advances cybersecurity scholarship by identifying **non-technical sources of cyber risk** rooted in governance structure. It explains why investments in tools and controls often fail to reduce exposure when accountability is fragmented.

For practitioners, the analysis informs governance redesign and accountability clarification. For executives and boards, it underscores the importance of integrated oversight mechanisms. For policymakers, it suggests that compliance-focused approaches may be insufficient without governance alignment (CISA, 2024; NIST, 2024).

8. Organization of the Article

The article progresses from governance theory and organizational context to a conceptual analysis of fragmentation-driven blind spots, followed by governance implications and directions for future research.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

9. Governance Fragmentation and Cybersecurity Blind Spots

Siloed governance design produces cybersecurity blind spots in predictable ways. Responsibility for risk is diffused across units, with partial visibility; reporting emphasizes local metrics rather than system-level exposure; and escalation pathways are unclear.

Standardized cybersecurity assessments often reveal these blind spots indirectly. Assessment outputs may identify gaps that no single unit claims ownership of addressing. Without governance mechanisms to integrate findings and assign accountability, assessments expose problems without resolving them (CISA, 2024; Mengnjo, 2026).

10. Implications for Governance and Practice

Reducing cybersecurity blind spots requires governance integration rather than incremental improvements in control. Organizations must clarify ownership of cross-functional risks, establish integrative oversight structures, and ensure that assessment outputs inform executive decision-making (Boyens et al., 2022; Shawe, 2026).
Cybersecurity governance should be treated as an enterprise risk function with clear accountability, escalation authority, and board visibility.

11. Limitations and Future Research

This study is conceptual and does not present empirical case data. Future research should examine governance fragmentation through organizational mapping, assessment outcomes, and longitudinal case studies across critical infrastructure sectors (Mengnjo, 2026).

12. Limitations and Boundary Conditions

This article is conceptual and does not present primary case-study data or interview findings. While healthcare and energy sectors provide contextual grounding, the governance fragmentation dynamics described here may manifest differently across other critical infrastructure domains.

The analysis focuses on structural accountability rather than technical vulnerability assessment. Future empirical research may examine specific organizational case studies to validate the interaction among governance fragmentation, assessment outputs, incident response, and board oversight processes.

13. Conclusion

Cybersecurity blind spots in critical infrastructure organizations are not random failures or isolated technical oversights. They are predictable outcomes of fragmented governance structures that diffuse responsibility and obscure accountability. Reconceptualizing cybersecurity risk as a governance problem provides a stronger foundation for reducing systemic exposure and strengthening infrastructure resilience (CISA, 2024; NIST, 2024).

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Authorship Statement

Dr. Robb Shawe and Dr. Gilbert Mengnjo jointly conceptualized the research orientation and governance perspective of this manuscript. Dr. Mengnjo contributed practitioner expertise spanning more than 15 years in cybersecurity governance, enterprise risk management, regulatory compliance, and healthcare information security.

Dr. Shawe contributed a multidisciplinary scholarly synthesis integrating critical infrastructure protection, cybersecurity governance, organizational resilience, and socio-technical systems theory. Dr. Shawe also led the development of the conceptual framing, literature integration, and manuscript preparation.

Both authors collaborated in refining the analytical framework, reviewing the manuscript, and approving the final version for submission.

This manuscript forms part of a broader **scholarly program of research** examining cybersecurity governance, risk management maturity, and resilience across critical infrastructure and organizational ecosystems.

Author Note and Copyright Statement

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.

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.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

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.

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

Boyens, J. M., Paulsen, C., Bartol, N., Winkler, K., & Gabel, O. (2022). *Cybersecurity supply chain risk management practices for systems and organizations* (NIST SP 800-161 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1

Cybersecurity and Infrastructure Security Agency. (2024). *Cyber Security Evaluation Tool (CSET®).* https://www.cisa.gov/cset

Mengnjo, G. B. (2026). *Assessing healthcare supply chain cybersecurity using the Cyber Security Evaluation Tool (CSET®) (Unpublished doctoral dissertation).* Capitol Technology University.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* https://www.nist.gov/cyberframework

Shawe, R. (2025). *Exploring smart grid technologies' impact on sustainable energy management in New York State* (Publication No. 32284053) [Doctoral dissertation, Capitol Technology University]. ProQuest Dissertations & Theses Global.

U.S. Department of Energy. (2022). *Cybersecurity Capability Maturity Model (C2M2), Version 2.1.* https://www.energy.gov/cybersecurity-capability-maturity-model-c2m2