International Journal of Advanced Engineering and Management Research

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Supply Chain Cybersecurity as an Emergent System Property in Critical Infrastructure

Dr. Robb Shawe (Lead Author)
Dr. Gilbert B. Mengnjo (Co-Author)
Capitol Technology University, Department of Critical Infrastructure, 11301 Springfield Road, Laurel, MD 20708, USA

doi.org/10.51505/ijaemr.2026.11209 URL: http://dx.doi.org/10.51505/ijaemr.2026.11209

Received: Mar 06, 2026 Accepted: Mar 17, 2026 Online Published: Mar 23, 2026

Abstract

Supply chain cybersecurity in critical infrastructure is commonly framed as a third-party risk management problem addressed through vendor assessments, contractual controls, and compliance checklists. While these mechanisms provide necessary baseline assurance, they are insufficient to detect and mitigate systemic cyber risk in highly interdependent infrastructure ecosystems. In sectors such as healthcare and energy, cybersecurity risk increasingly emerges from the structure of interdependencies among internal organizational units, shared digital services, and tightly coupled supplier relationships rather than from isolated vendor weaknesses. This conceptual article reframes supply chain cybersecurity as an emergent system property shaped by dependency topology, coupling strength, and governance alignment. Drawing on systems theory, interdependence, and cascading failure concepts, the paper explains why transactional, vendor-centric approaches routinely underestimate exposure and fail to anticipate propagation pathways. A systems-informed governance perspective is proposed to support executive oversight, resilience planning, and policy development in critical infrastructure supply chains. The contribution advances theoretical understanding while offering a practical governance lens for leaders seeking to reduce cascading cyber risk across complex socio-technical ecosystems.

Keywords: Supply chain cybersecurity; emergent risk; interdependence; cascading failure; critical infrastructure; healthcare supply chains; energy systems; governance; resilience

1. Introduction

This article argues that standardized cybersecurity assessments function most effectively as instruments for revealing emergent, system-level risk arising from interdependence, rather than as tools for diagnosing organizational governance failure or executive decision-making practices. Supply chain cybersecurity has emerged as a central concern for critical infrastructure sectors as organizations increasingly rely on digitally integrated ecosystems to sustain operations. Healthcare delivery systems, energy generation and distribution networks, and other

Vol. 11, No. 02; 2026

ISSN: 2456-3676

infrastructure domains depend on complex networks of suppliers, service providers, internal units, and shared platforms that collectively ensure service continuity. While these interconnected supply chains improve efficiency and scalability, they also expand the cyber-attack surface and increase the potential for cascading disruption.

The dominant framing of supply chain cybersecurity treats risk as a vendor-level problem managed through third-party risk assessments, contractual clauses, and compliance verification. In this view, improving supplier controls is assumed to reduce supply chain cyber risk proportionally. However, real-world incidents increasingly demonstrate that disruptions propagate across organizational boundaries through shared services, privileged access pathways, and tightly coupled dependencies—even when most vendors appear compliant.

This systems-and-interdependence orientation is consistent with sector-specific doctoral research emphasizing ecosystem coupling, governance, and cascading risk dynamics (Mengnjo, 2026; Shawe, 2026). Supply chain cybersecurity risk in critical infrastructure, therefore, cannot be adequately understood as the sum of individual vendor postures. Instead, risk emerges from interdependence—the relationships, interfaces, and coupling among organizational units and suppliers that produce **system-level risk behavior** and enable cyber events to cascade across the ecosystem. The purpose of this article is to reconceptualize supply chain cybersecurity as an emergent system property and to establish a conceptual foundation for governance approaches that address systemic exposure rather than isolated entities.

This manuscript constitutes a segment of an extensive research initiative investigating the governance interpretation of cybersecurity evaluation outputs within critical infrastructure settings. The series explores how cybersecurity assessments, maturity models, and governance frameworks impact organizational learning, risk prioritization, and resilience in complex socio-technical systems. By integrating multidisciplinary academic analysis with practitioner-informed perspectives, the research aims to elucidate how governance design, regulatory frameworks, and organizational accountability influence the efficacy of cybersecurity risk management and operational resilience.

1.1 Methodological Orientation

This article employs a qualitative conceptual analysis informed by systems theory and interdependence frameworks. Using healthcare and energy infrastructure contexts as comparative illustrations, the study interprets supply chain cybersecurity risk as an emergent property arising from coupling, dependency chains, and governance design. The analysis synthesizes maturity assessment outputs, sectoral governance structures, and inter-organizational relationships to construct a system-level risk interpretation model. The intent is theoretical refinement rather than empirical generalization.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

2. Background and Context

2.1 Dominant supply chain cybersecurity framing

In this article, the term cybersecurity assessment outputs refers to the structured findings generated by standardized cybersecurity assessment instruments, including maturity model results, domain scores, and governance-relevant evidence artifacts. Supply chain cybersecurity literature and practice have traditionally emphasized third-party risk management (TPRM). Organizations assess suppliers through questionnaires, audits, and attestations designed to verify alignment with baseline security requirements. This approach aligns with established supply chain risk management guidance and supports regulatory expectations for due diligence and documentation (Boyens et al., 2022).

While necessary, this framing privileges transactional assurance over systemic understanding. Vendor controls are often evaluated independently of how suppliers interact with mission-critical processes, shared platforms, or other suppliers. As a result, organizations may achieve a strong compliance posture without reducing the likelihood or impact of cascading cyber events. 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).

2.2 Systems, interdependence, and emergence

Systems theory emphasizes that complex systems exhibit emergent behavior—outcomes produced by interactions among components rather than by the properties of individual elements. Interdependence exists when the functioning of one component affects others, creating pathways through which disruption can propagate.

In digitally integrated supply chains, interdependence is intensified by shared identity systems, cloud services, remote access mechanisms, integrated procurement platforms, and vendor-managed technologies. Cybersecurity risk in such environments is a **system-level risk property** shaped by dependency structure and coupling strength rather than a simple aggregation of vendor weaknesses.

Recent cyber incidents demonstrate how cascading cyber risk emerges from interdependent supply chain environments. For example, disruptions involving third-party software providers have propagated across multiple organizations simultaneously due to shared platforms and centralized service dependencies. In such cases, the compromise of a single vendor created downstream operational impacts across healthcare providers, logistics networks, and financial systems. These events illustrate that cybersecurity risk is not confined to individual organizational boundaries but is amplified through interdependence and coupling among entities. Even when individual organizations maintain compliant cybersecurity postures, shared dependencies may introduce systemic vulnerabilities that enable cyber incidents to cascade across the broader ecosystem.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

2.3 Gap in literature and practice

Despite growing recognition of systemic cyber risk, scholarship on supply chain cybersecurity has rarely treated it explicitly as an emergent system property. Governance frameworks often assume linear risk reduction through incremental control improvements, overlooking non-linear dynamics such as weakest-link effects and propagation pathways. This gap limits both theoretical development and the effectiveness of practical governance in critical infrastructure contexts.

3. Problem Statement

It is not known how cybersecurity risk emerges from interdependent relationships within critical infrastructure supply chains beyond individual vendor controls, resulting in governance approaches that under-detect cascading exposure and over-rely on transactional, compliance-based mechanisms.

4. Purpose of the Study

The purpose of this qualitative, conceptual analysis is to examine supply chain cybersecurity as an emergent system property within critical infrastructure contexts, with particular emphasis on healthcare and energy ecosystems, and to propose a systems-informed governance perspective that supports resilience-oriented oversight and decision-making.

5. Research Questions

RQ1: How does interdependence shape cybersecurity risk across critical infrastructure supply chains?

RQ2: What system-level vulnerabilities emerge from coupling among organizational units and suppliers?

RQ3: Why do traditional vendor-centric controls fail to address emergent and cascading cyber risk?

To address the research questions, this study applies a systems-based analytical lens, interpreting supply chain cybersecurity risk as an emergent property of interdependence, coupling, and governance alignment. Rather than evaluating individual vendor controls in isolation, the analysis examines how relationships among organizational units, shared services, and supplier networks produce system-level risk behavior. Each research question is considered through the interaction of dependency topology, coupling intensity, and propagation pathways, enabling a structured interpretation of how cybersecurity risk emerges and amplifies across interconnected infrastructure environments.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

6. Theoretical and Conceptual Framework

This analysis integrates systems theory, interdependence, and cascading-failure concepts to interpret supply-chain cybersecurity at the ecosystem level. Systems theory provides the foundation for understanding emergence and non-linear behavior. Interdependence theory explains how shared functions and mutual reliance amplify exposure. Cascading failure logic illustrates how localized cyber events propagate across tightly coupled systems.
Together, these perspectives support a conceptual framework in which supply chain cybersecurity is understood as a function of dependency topology, coupling strength, and governance alignment. This framing shifts the analysis from individual suppliers to the structure of the supply chain ecosystem.

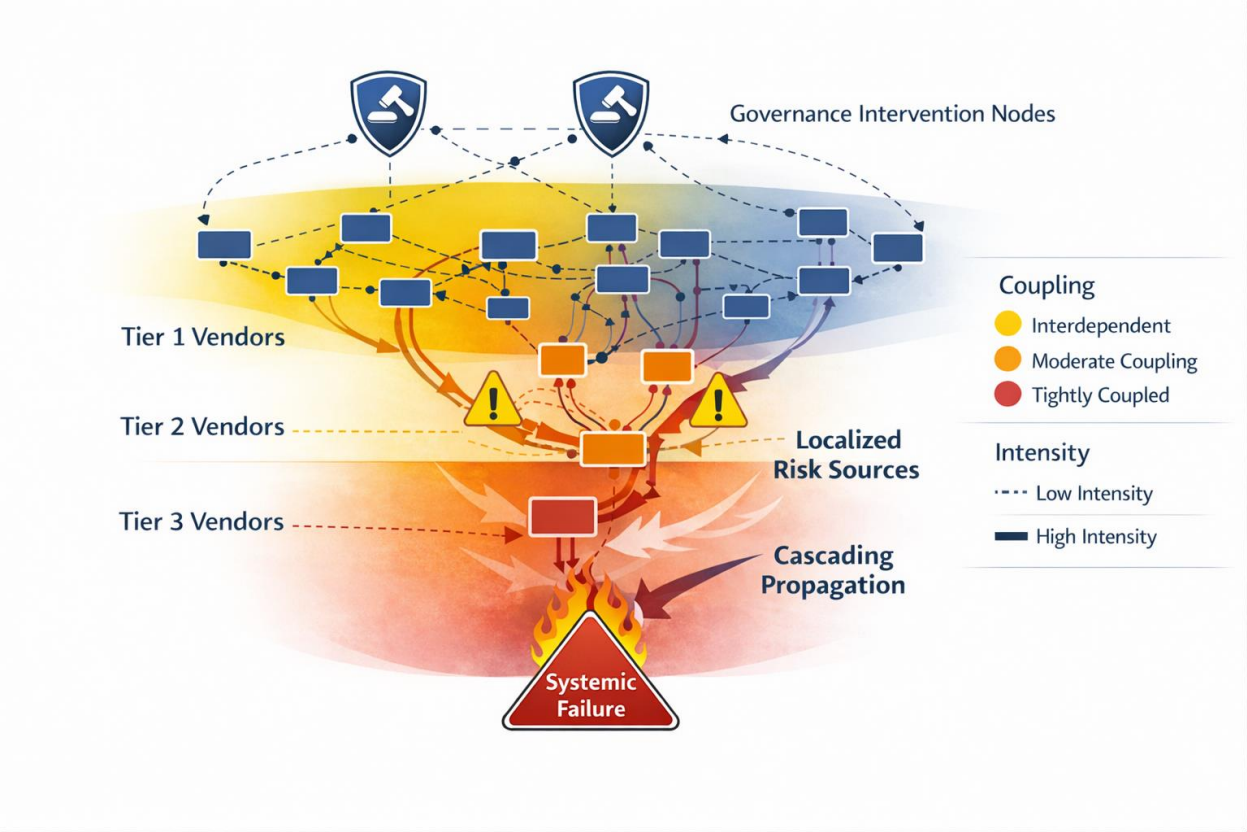
As conceptualized in Figure 1, supply chain cybersecurity risk emerges not from isolated vendor deficiencies but from the structural coupling and dependency intensity that characterize interdependent infrastructure networks.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Figure 1

Emergent Cyber Risk Across Interdependent Supply Chain Networks



Note. Author created. The figure depicts supply chain cybersecurity risk as an emergent property arising from interdependent vendor relationships across multiple tiers. Risk does not originate solely from isolated vendor weaknesses but emerges through coupling intensity, dependency chains, and cascading propagation pathways. Governance intervention nodes represent points at which oversight mechanisms may interrupt or mitigate risk amplification. The model is conceptual and intended to illustrate system-level risk dynamics rather than to quantify incident probability or network failure rates.

Accordingly, supply chain cybersecurity risk must be governed as a function of system structure and interdependence rather than as a collection of isolated vendor attributes, reinforcing the need for network-aware governance strategies.

The multi-tier structure illustrated in the model demonstrates how localized vulnerabilities within lower-tier vendors may propagate upward through tightly coupled operational pathways, particularly when oversight mechanisms focus narrowly on first-tier compliance validation. The interaction between coupling intensity and governance design determines whether vulnerabilities

Vol. 11, No. 02; 2026

ISSN: 2456-3676

remain contained or escalate into cascading disruption. In this configuration, risk amplification is a function of system topology and coordination architecture rather than of any single vendor's maturity level. Consequently, effective supply chain cybersecurity governance must account for network-level interdependence rather than relying exclusively on transactional vendor assessments.

Table 1 summarizes the core system-level concepts that define supply chain cybersecurity as an emergent property and clarifies their corresponding governance implications within interdependent critical infrastructure environments.

Table 1

Key Concepts in Emergent Supply Chain Cybersecurity Risk

Concept	Definition	Governance Implication
Interdependence	Mutual reliance among organizational units and suppliers	Requires cross-entity visibility
Coupling	Degree of connection between systems and processes	High coupling increases propagation risk
Emergent Risk	Risk arising from system interactions rather than individual failures	Cannot be managed through vendor controls alone
Cascading Failure	Propagation of disruption across interconnected systems	Requires resilience-focused governance
Dependency Topology	Structural arrangement of supply chain relationships	Must be mapped and monitored

Note. Author created. The table summarizes key system-level concepts that define supply chain cybersecurity risk as an emergent property in interdependent infrastructure environments.

Collectively, these system-level concepts demonstrate that supply chain cybersecurity risk is not an aggregation problem but a structural property of interdependence, requiring governance approaches that account for the interactions and dependencies among system components rather than isolated vendor attributes.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

7. Significance of the Study

This study makes a distinct contribution to the cybersecurity governance and supply chain risk management literature by explicitly conceptualizing supply chain cybersecurity as an emergent system property rather than as an aggregation of vendor-level risks. While existing approaches emphasize third-party risk management and compliance-based controls, this analysis introduces a systems-informed perspective that accounts for interdependence, coupling intensity, and cascading failure dynamics. By reframing cybersecurity risk as a function of system structure and interaction, the study extends current theoretical models and provides a governance-oriented framework for understanding and mitigating systemic cyber risk in critical infrastructure environments.

8. Organization of the Article

The article progresses from a review of dominant supply chain cybersecurity framing to a systems-based reconceptualization of risk emergence. It then develops theoretical foundations, articulates governance implications, and concludes with directions for future research and practice focused on resilience and on reducing systemic risk.

9. Implications for Governance and Practice

Reframing supply chain cybersecurity as an emergent property has significant governance implications. Executive oversight must extend beyond vendor inventories to include dependency topology, coupling criticality, and cross-entity coordination. Assessment tools such as the Cyber Security Evaluation Tool (CSET®) can support governance visibility by providing standardized insight into preparedness across interdependent units, but their value depends on interpretation through a systems lens (Cybersecurity and Infrastructure Security Agency [CISA], 2024; Mengnjo, 2026; Shawe, 2026).

Organizations should prioritize governance mechanisms that identify high-coupling dependencies, elevate assurance requirements for critical interfaces, and invest in weakest-link improvement strategies that yield disproportionate resilience benefits.

10. Limitations and Future Research

This study advances a conceptual and governance-oriented interpretation of supply chain cybersecurity as an emergent system property. As such, the analysis does not empirically model cascading cyber-failure probabilities, nor does it provide quantitative network simulations of inter-organizational dependency chains. The sectoral illustrations drawn from healthcare and energy infrastructure contexts are interpretive and governance-analytic in nature, rather than statistically generalizable representations of supply chain risk across all critical infrastructure sectors.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Additionally, the study does not evaluate real-time operational telemetry or incident-level data to validate the precise mechanics of propagation across interdependent nodes. Instead, it synthesizes documented maturity outputs, governance structures, and interdependence dynamics to refine theoretical understanding. The conceptual model should therefore be interpreted as a governance framework for risk interpretation rather than as a predictive model of cyber event occurrence.

Future research may extend this work through quantitative network mapping, dependency modeling, or empirical case studies examining cascading cyber incidents across sector-specific supply chains. Comparative analyses involving additional infrastructure sectors may also help clarify the conditions under which emergent risk amplification is most pronounced. Such empirical extensions would further test and operationalize the governance-based framework proposed in this study.

11. Conclusion

Supply chain cybersecurity in critical infrastructure cannot be effectively governed as a vendor compliance problem alone. Risk emerges from interdependence—shared services, tightly coupled processes, and propagation pathways that enable localized cyber events to cascade across ecosystems. Reconceptualizing supply chain cybersecurity as an **ecosystem-level risk characteristic** provides a stronger theoretical foundation and a more effective governance lens.

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, the integration of the literature, and the preparation of the manuscript.

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.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

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.

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

Vol. 11, No. 02; 2026

ISSN: 2456-3676

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