International Journal of Advanced Engineering and Management Research

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Cross-Unit Cybersecurity Variability as a Driver of Systemic Risk in Critical Infrastructure Supply Chains

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.2026.11208 URL: http://dx.doi.org/10.51505/ijaemr.2026.11208

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

Abstract

Cybersecurity risk in critical infrastructure sectors is commonly evaluated using enterprise-level indicators that aggregate performance across organizational units and supply chain partners. While aggregation simplifies oversight and reporting, it obscures meaningful variation in cybersecurity capability that can amplify systemic risk in interdependent systems. This article examines cross-unit cybersecurity variability as an underappreciated yet decisive driver of systemic cyber risk in critical infrastructure supply chains. Drawing on assessment-based evidence from healthcare supply chains and on governance and resilience analyses from energy and smart-grid infrastructure contexts, the study reframes cybersecurity risk as a distributional phenomenon shaped by uneven capabilities, governance fragmentation, and interorganizational dependence. This analysis indicates that governance approaches relying on average maturity or compliance status can systematically underestimate exposure and weaken resilience planning. By foregrounding variability and weakest-link dynamics, this article advances cybersecurity governance theory and offers practical guidance for improving oversight, prioritization, and resilience across critical infrastructure ecosystems.

Keywords: cybersecurity governance; supply chain cybersecurity; systemic risk; interdependence; cybersecurity assessments; critical infrastructure; resilience

1. Introduction

Critical infrastructure sectors increasingly operate as interconnected ecosystems rather than as isolated organizations. Healthcare delivery systems, energy generation and distribution networks, and other essential services rely on digitally mediated supply chains composed of internal organizational units, vendors, service providers, and platform operators. These interdependencies improve efficiency and scalability but also introduce systemic cyber risk that extends beyond any single organizational boundary (Mengnjo, 2026; Shawe, 2026).

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Despite the growth of interdependence, cybersecurity governance and reporting practices continue to emphasize enterprise-level posture. Organizations routinely summarize cybersecurity performance through aggregate compliance indicators, maturity scores, or audit outcomes. While such indicators reduce technical complexity and facilitate executive reporting, they also mask uneven distribution of cybersecurity capability across organizational units and supply chain partners (Shawe, 2026). This distinction reframes cybersecurity risk from an aggregate condition to a distributional phenomenon, in which system-level exposure is determined by the weakest nodes within interdependent structures rather than by average organizational performance.

This article advances the argument that **cross-unit cybersecurity variability is itself a major contributor to systemic cyber risk** in critical infrastructure supply chains. When cybersecurity capability is unevenly distributed, the least mature units or partners disproportionately shape exposure, regardless of overall compliance status. In tightly coupled systems, localized weaknesses serve as entry points for cascading failures (Mengnjo, 2026; Boyens et al., 2022). While prior analyses of cybersecurity risk emphasize interdependence and cascading failure as drivers of systemic exposure, this study isolates cross-unit cybersecurity variability as a distinct governance problem. Specifically, it demonstrates that the distribution of cybersecurity capability—rather than interdependence alone—determines where systemic risk concentrates and how it propagates across interconnected infrastructure systems.

Building on doctoral research examining healthcare supply chain cybersecurity using structured assessment tools, and complementary doctoral work on governance and resilience in energy and smart-grid infrastructure, this study reframes cybersecurity risk from an averaged organizational attribute to a **distributional governance problem**. It demonstrates why prevailing governance approaches underestimate exposure and how assessment-informed visibility into variability can support more effective oversight and resilience planning.

This manuscript is part of an extensive research initiative that explores the governance interpretation of cybersecurity assessment outputs within critical infrastructure environments. The series analyzes how cybersecurity assessments, maturity models, and governance frameworks influence 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 impact the efficacy of cybersecurity risk management and operational resilience.

1.1 Methodological Orientation

This study adopts a qualitative, comparative governance analysis grounded in a cross-sector examination of healthcare supply chain cybersecurity and energy infrastructure systems. Rather than relying on quantitative maturity aggregation, the analysis interprets variability in cybersecurity posture across organizational units as a governance phenomenon. Documentary evidence, maturity outputs, and sector-specific contextual insights are examined through systems

Vol. 11, No. 02; 2026

ISSN: 2456-3676

and risk-distribution lenses to evaluate how uneven maturity generates systemic exposure. The approach is conceptual and analytic, intended to illuminate governance dynamics rather than to produce statistical generalizations.

2. Background and Context

2.1 Interdependence in critical infrastructure supply chains

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. Modern critical infrastructure sectors are defined by operational and digital interdependence. Healthcare organizations rely on electronic health records, cloud-hosted clinical platforms, connected medical devices, and third-party service providers to deliver care. Energy systems depend on interconnected generation assets, grid operators, vendors, and digital control technologies to maintain reliability and safety (Mengnjo, 2026; Shawe, 2026).

Comparable patterns of cybersecurity variability have also been observed across other critical infrastructure sectors, including transportation systems, financial services institutions, and water utilities. These sectors increasingly rely on interconnected digital supply chains and third-party service providers, creating conditions in which uneven cybersecurity maturity across organizational units can introduce systemic vulnerabilities that extend beyond individual organizational boundaries.

Research embedded in both authors' doctoral work emphasizes that cyber incidents in such environments rarely remain localized. Instead, disruptions propagate through shared data flows, trust relationships, and vendor dependencies, amplifying operational and system-wide exposure across the broader ecosystem (Mengnjo, 2026; Shawe, 2026). As a result, cybersecurity risk emerges at the **system level**, not merely within individual organizations.

2.2 Governance challenges in distributed environments

Governance in interdependent environments is inherently fragmented. Responsibility for cybersecurity is distributed across information technology functions, operational units, procurement processes, compliance offices, and executive leadership. Across supply chains, governance extends beyond organizational boundaries to include vendors and service providers over which direct control is limited (Mengnjo, 2026).

Doctoral research in healthcare supply chain cybersecurity demonstrates that organizations often rely on vendor attestations, contractual clauses, or baseline compliance requirements that offer limited insight into their actual cybersecurity capabilities (Mengnjo, 2026). Similarly, governance analysis in energy infrastructure highlights that alignment with high-level frameworks does not guarantee consistent implementation across system components (Shawe, 2026). Together, these analyses point to a shared governance gap: leaders lack reliable,

Vol. 11, No. 02; 2026

ISSN: 2456-3676

comparable information on where cybersecurity capabilities are weakest across their operational and supply chain ecosystems. 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).

Recent research and federal guidance further emphasize the importance of addressing cybersecurity governance across interconnected supply chains. For example, the National Institute of Standards and Technology has developed comprehensive guidance on information and communication technology supply-chain risk management to help organizations manage cybersecurity dependencies across vendors and partner organizations (Boyens et al., 2022). Similarly, the Cybersecurity and Infrastructure Security Agency (CISA, 2023) has highlighted the need for coordinated cybersecurity governance practices across critical infrastructure ecosystems to mitigate systemic cyber risk. These frameworks reinforce the importance of addressing cybersecurity variability across organizational units as a key component of strengthening supply-chain resilience.

3. Problem Statement

Despite widespread adoption of cybersecurity frameworks, maturity models, and assessment tools, it remains unclear how cross-unit variability in cybersecurity capability contributes to systemic cyber risk in critical infrastructure supply chains. Existing governance approaches rely heavily on enterprise-level or compliance-based indicators that obscure internal and interorganizational disparities, limiting leaders' ability to identify weakest-link exposure and to prioritize interventions that meaningfully improve resilience (Mengnjo, 2026; Shawe, 2026).

4. Purpose of the Study

The purpose of this qualitative, governance-focused analysis is to examine how cybersecurity capabilities vary across organizational units and supply chain partners in critical infrastructure environments and how this variability amplifies systemic cyber risk. By integrating assessment-based evidence from healthcare supply chains with governance and resilience insights from energy infrastructure contexts, the study seeks to demonstrate the importance of visibility into variability for effective cybersecurity governance and resilience planning (Mengnjo, 2026; Shawe, 2026).

5. Research Questions

This study is guided by the following research questions:

1. How does cybersecurity capability vary across organizational units and supply chain partners within critical infrastructure sectors?
2. In what ways does cross-unit variability amplify systemic cyber risk in interdependent environments?
3. How do prevailing governance and assessment practices obscure or reveal this variability?

Vol. 11, No. 02; 2026

ISSN: 2456-3676

6. Conceptual and Theoretical Framework

This study integrates systems theory, governance theory, and supply chain risk management principles to conceptualize cybersecurity risk as a distributional phenomenon.
Systems and interdependence theory emphasize that risk emerges from relationships among components rather than from isolated failures, particularly in tightly coupled cyber-physical systems (Shawe, 2026). Governance theory further underscores that effective oversight depends on the availability of comparable and interpretable information across organizational domains, enabling leaders to allocate resources and enforce accountability (Shawe, 2026).

Supply chain risk management theory highlights weakest-link dynamics, whereby the least capable actors disproportionately shape system-level exposure. This dynamic is consistently observed in healthcare supply chain cybersecurity assessment results, in which low-maturity vendors and organizational units are primary sources of systemic vulnerability (Mengnjo, 2026; Boyens et al., 2022).

7. Assessment-Based Evidence of Cross-Unit Variability

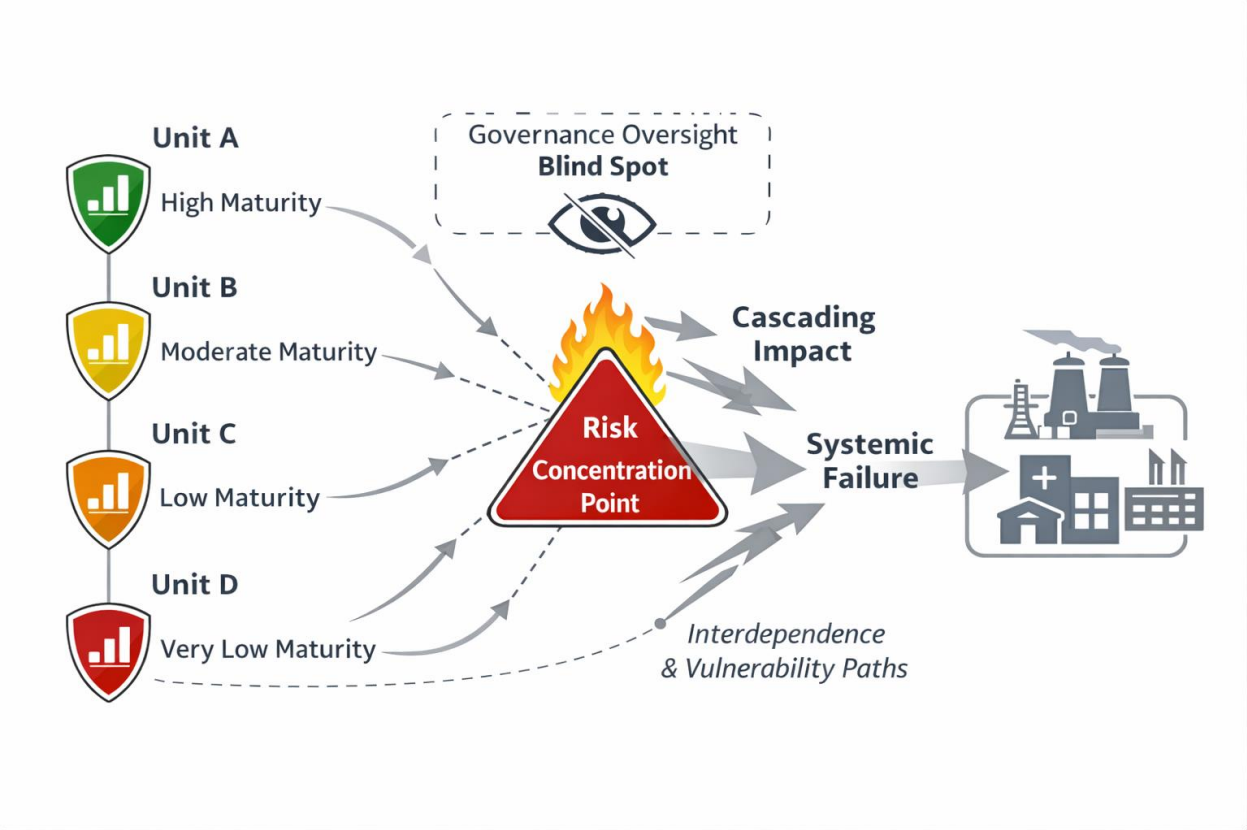
As illustrated in Figure 1, uneven cybersecurity maturity across organizational units can converge at interdependence nodes, producing concentrated system-level exposure that remains obscured under enterprise-level averages.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Figure 1

Systemic Risk Amplification Through Cross-Unit Cybersecurity Variability



Note. Author created. The figure illustrates how uneven cybersecurity maturity across organizational units can generate concentrated systemic risk within interdependent infrastructure systems. Units with varying maturity levels contribute different levels of vulnerability exposure, which may converge at points of operational interdependence. Without effective governance oversight capable of detecting cross-unit variability, localized weaknesses may amplify into cascading impacts and broader systemic failure across critical infrastructure contexts. The model is conceptual and intended to depict governance-related risk dynamics rather than empirical magnitude.

Taken together, these dynamics reinforce that systemic cyber risk is not determined by aggregate organizational posture, but by the distribution of capability across interdependent units, thereby necessitating governance approaches that explicitly identify and address weakest-link exposure.

The distributional nature of cybersecurity maturity across organizational units demonstrates that enterprise-wide averages do not determine systemic exposure, but rather the relative position of the weakest operational nodes within interdependent structures. Units operating at lower maturity

Vol. 11, No. 02; 2026

ISSN: 2456-3676

levels may introduce disproportionate vulnerability when tightly coupled to higher-functioning domains, particularly where information flows, shared services, or critical process dependencies exist. In such configurations, localized weaknesses can propagate across organizational boundaries, amplifying risk through propagating operational pathways. Consequently, governance mechanisms that rely primarily on aggregate maturity indicators may fail to detect concentrated exposure points embedded within cross-unit variability.

Recent cyber incidents have demonstrated how uneven cybersecurity maturity across organizational units can amplify systemic risk in critical infrastructure supply chains. For example, ransomware incidents affecting healthcare networks have often originated through compromised vendor or departmental systems with weaker cybersecurity controls. While enterprise governance frameworks may establish cybersecurity policies at the organizational level, operational units frequently vary in their implementation maturity due to differences in staffing, resources, or local governance practices. This variability can create hidden vulnerabilities that propagate across interconnected supply chain networks. Similar patterns have been observed in energy utilities and transportation infrastructure, where vendor or subsidiary organizations operate with different cybersecurity maturity levels, allowing adversaries to exploit weaker nodes within the broader ecosystem.

7.1 Structured cybersecurity assessments as visibility mechanisms

Structured cybersecurity assessments provide a mechanism for revealing cross-unit variability that is invisible in aggregated reporting. The Cybersecurity Evaluation Tool (CSET) is a structured assessment instrument maintained by the Cybersecurity and Infrastructure Security Agency (CISA) to evaluate the alignment of cybersecurity practices and maturity in operational environments. Application of CSET across healthcare organizations reveals substantial variation in practices for asset management, monitoring, incident response, and third-party risk management (Cybersecurity and Infrastructure Security Agency [CISA], 2024; Mengnjo, 2026). Comparable variability is observed in energy and smart-grid infrastructure contexts, where the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2) and related maturity-aligned governance approaches reveal uneven implementation of cybersecurity and resilience practices across system components (U.S. Department of Energy [DOE], 2022; Shawe, 2026). In both sectors, assessment results indicate that systemic exposure is often shaped by a limited number of low-maturity entities rather than by average performance.

7.2 Variability and weakest-link exposure

Assessment-based evidence indicates that weakest-link dynamics frequently drive systemic cyber risk. Low-maturity units or vendors can serve as points of entry or disruption, compromising broader system operations, even when enterprise-level indicators suggest an adequate posture (Mengnjo, 2026; Shawe, 2026). Governance mechanisms that rely on average scores or compliance thresholds fail to identify these weak points, creating a false sense of security.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

8. Governance Implications of Cross-Unit Variability

8.1 Limits of compliance-centric governance

Compliance-centric governance approaches emphasize documentation and the presence of baseline controls. While necessary, these mechanisms do not capture operational variability across supply chains. As demonstrated in healthcare cybersecurity governance, organizations may satisfy formal requirements while remaining vulnerable to disruption originating from poorly governed vendor relationships (Mengnjo, 2026).

8.2 Reframing governance around variability

Effective cybersecurity governance in interdependent environments requires mechanisms that enable cross-unit and cross-vendor comparisons, identify outliers and weakest performers, and support the targeted prioritization of remediation efforts. Governance reporting can be strengthened by mapping assessment outputs to the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (CSF 2.0) outcomes to improve interpretability for executive decision-making (National Institute of Standards and Technology [NIST], 2024; Shawe, 2026).

Table 1

Governance Strategies for Reducing Cross-Unit Cybersecurity Variability

Governance Challenge	Organizational Condition	Governance Strategy
Uneven cybersecurity maturity across organizational units	Departments interpret cybersecurity frameworks inconsistently	Establish centralized cybersecurity governance oversight
Vendor cybersecurity disparities	Third-party suppliers operate at lower maturity levels	Require standardized cybersecurity assessments across vendors
Fragmented risk visibility	Cyber risk is reported independently across units	Integrate cybersecurity into enterprise risk management (ERM)
Resource imbalance across units	Smaller units lack cybersecurity expertise	Implement shared services or centralized security operations
Weakest-link exposure	Low-maturity units create systemic risk pathways	Prioritize remediation based on the lowest maturity nodes

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Note. Author created. The table summarizes governance strategies organizations may adopt to reduce cybersecurity variability across organizational units and strengthen systemic resilience within critical infrastructure supply chains.

Collectively, these governance strategies demonstrate that reducing systemic cyber risk requires shifting from uniform compliance approaches toward targeted interventions that address variability at its most critical points within interdependent systems.

9. Implications for Critical Infrastructure Resilience

Reframing cybersecurity risk as a distributional phenomenon has direct implications for resilience planning. Evidence from both healthcare and energy infrastructure contexts indicates that improving the cybersecurity capability of the weakest units yields disproportionate gains in system-level resilience (Mengnjo, 2026; Shawe, 2026). This finding aligns with maturity-based governance frameworks that emphasize continuous improvement and risk-informed prioritization (DOE, 2022; NIST, 2024).

10. Contribution and Significance

This article contributes to the cybersecurity governance and supply chain risk management literature by explicitly identifying cross-unit cybersecurity variability as a driver of systemic cyber risk in critical infrastructure. It extends existing frameworks by integrating assessment-based evidence with governance and resilience theory, demonstrating how visibility into variability can support more effective oversight and system-level risk reduction (Mengnjo, 2026; Shawe, 2026).

By explicitly modeling cybersecurity risk as a distributional phenomenon shaped by variability rather than average performance, this study extends prevailing governance frameworks that implicitly assume uniform capability across interdependent systems.

11. Limitations and Boundary Conditions

This study is conceptual and comparative, drawing on governance analysis across healthcare and energy contexts. It does not quantify risk amplification effects nor provide sector-wide statistical validation. The cross-sector illustrations are bounded by available documentary and assessment-derived evidence. Findings should therefore be interpreted as governance-analytic insights rather than empirical prevalence claims. Future research may employ mixed-method or quantitative modeling approaches to examine the measurable impact of cross-unit variability on incident frequency and severity.

12. Conclusion

Cybersecurity risks in critical infrastructure supply chains cannot be effectively managed solely through aggregated indicators. Cross-unit variability—amplified by interdependence—creates

Vol. 11, No. 02; 2026

ISSN: 2456-3676

systemic exposure that governance mechanisms must confront explicitly. By leveraging standardized assessments and maturity-aligned governance frameworks to surface and address variability, organizations can strengthen oversight, improve resilience, and reduce the likelihood of cascading cyber failures across critical infrastructure ecosystems (Mengnjo, 2026; Shawe, 2026). This analysis suggests that governance reporting and oversight should shift from enterprise-level averages toward distributional visibility and weakest-link identification.

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.

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.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

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. (2023). *Cybersecurity supply chain risk management guide.* U.S. Department of Homeland Security.

Cybersecurity and Infrastructure Security Agency. (2024). *Cyber Security Evaluation Tool (CSET®).* Retrieved 27 January 2026, from https://www.cisa.gov/cset

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

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). 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