Journal of Economich, Technology and Business (JETBIS)
Volume 4, Number 9 September 2025
p-ISSN 2964-903X; e-ISSN 2962-9330

Assessing Cybersecurity Strategies for Critical Infrastructure Protection in the Era of Digitalization

Septien Dwi Savandha
Universidad Tecnológica Latinoamericana en Línea (UTEL), USA
Email: dwisavandha9@gmail.com
*Correspondence: dwisavandha9@gmail.com

KEYWORDS:
Cybersecurity Strategies; Critical Infrastructure; Digitalization; Organizational Barriers; Ransomware

ABSTRACT

The protection of critical infrastructure in the digital era faces escalating cyber threats, most notably ransomware, necessitating rigorous cybersecurity strategies. This study aims to assess the current cybersecurity approaches employed in critical infrastructure sectors, determine key vulnerabilities, and highlight pressing implementation barriers amid advancing digitalization. Employing a descriptive qualitative research design, the study engaged purposively selected cybersecurity professionals, IT managers, and policymakers across key infrastructure sectors. Data were collected via semi-structured interviews and document analysis, followed by thematic analysis using both inductive and deductive coding to extract salient organizational and technical themes. The analysis revealed that ransomware poses the most frequent and impactful threat, while organizations predominantly rely on traditional controls such as network segmentation and employee training. Advanced dynamic measures, such as real-time monitoring, remain underutilized. Organizational barriers—including resource constraints, regulatory ambiguity, and legacy system complexity—were consistently reported as major hindrances to effective cybersecurity implementation. These findings underline a critical need for targeted innovation, workforce development, and policy reform to bridge the gap between threat sophistication and current defense practices. The study advances theoretical understanding of cyber risk management in complex infrastructures and offers practical recommendations for future policy and organizational strategy. Study limitations include qualitative scope and sample representativeness, suggesting the need for longitudinal and sector-wide quantitative research.

INTRODUCTION

This study investigates the relationship between digitalization processes (independent variable) and cybersecurity effectiveness in critical infrastructure (dependent variable), while examining how organizational barriers and strategic choices mediate this relationship (Kilani, 2020; Oroni & Fu, 2023; Sulistio, 2023; Val et al., 2025). The rapid advancement of digital technologies has fundamentally transformed the way critical infrastructure systems operate, magnifying both their efficiency and vulnerability to cyber threats (Ajayi et al., 2025; Djenna et al., 2021; Riggs et al., 2023). As nations increasingly depend on interconnected digital platforms for the management of essential services—such as energy, transportation, healthcare, and finance—these infrastructures have become prime targets for sophisticated cyberattacks perpetrated by state and non-state actors (Adeyeri & Abroshan, 2024; Durojaye & Raji, 2022; Rees & Rees, 2023). Recent incidents have demonstrated the devastating impact that ransomware campaigns, supply chain attacks, and exploits

of industrial control systems (ICS) can have on societal stability and economic continuity (Asiri et al., 2023; Ma et al., 2025; Makrakis et al., 2021).

Emerging research highlights a discernible shift in the threat landscape, driven by artificial intelligence, expanding Internet of Things (IoT) environments, and hybrid physical-cyber attacks (Kilani, 2020; Oroni & Fu, 2023; Sulistio, 2023). For example, Rajender Pell Reddy (2025) argues that the fusion of old-generation and next-generation security measures is essential to protect national assets in the digital age, emphasizing current risks and calling for immediate solutions through layered security strategies that combine traditional controls with innovative digital defenses. However, Reddy's framework remains largely conceptual and does not empirically validate whether such layered approaches effectively reduce breach incidents in operational environments (Jeyaram & Muthukumaravel, 2024; Owobu et al., 2022; Reddy et al., 2023). Meanwhile, Zatonatskiy et al. (2025) examine the need for adapting international regulatory standards—such as those of the European Union—for effective digitalization and cyber protection, focusing on the importance of strategic planning, regulatory harmonization, and human capital development in building resilient infrastructures. While their policy analysis is comprehensive, it lacks empirical evidence from infrastructure operators regarding implementation challenges in diverse regulatory contexts (Ahmadi-Assalemi et al., 2020; Zaydi et al., 2025; Zhang et al., 2022). Further, the Carnegie Endowment's Global Technology Summit (2025) identifies key challenges, including gaps in international cooperation, inconsistent definitions of critical infrastructure, and persistent vulnerabilities in hardware supply chains, demanding increased collaboration among governments, the private sector, and global partners. Yet this policy discourse does not address the organizational and resource barriers that prevent coordinated responses at the operational level.

Despite these efforts, a significant research gap remains in the empirical validation and practical effectiveness of cybersecurity strategies tailored for critical infrastructure environments (Ani et al., 2019; Karabacak et al., 2016; Val et al., 2025). López-Morales et al. (2025) present a systematic review indicating that many proposed defensive measures lack rigorous scientific assessment and reproducibility, casting doubt on their reliability and real-world applicability in industrial settings. Most current frameworks focus on concept-level solutions or single-domain controls, with limited guidance on integrating real-time monitoring, asset visibility, and coordinated incident response—a gap further exposed by increasing breaches and operational disruptions in recent years. This research gap is crucial because without empirical validation of cybersecurity strategies in real-world critical infrastructure settings, policymakers and operators cannot confidently allocate limited resources to the most effective defensive measures. The consequences of ineffective strategy selection are severe: continued operational disruptions, escalating financial losses, erosion of public trust, and potential cascading failures across interconnected infrastructure sectors. As digitalization accelerates, the window for establishing evidence-based protective frameworks narrows, making immediate empirical research essential to prevent long-term systemic vulnerabilities that could compromise national security and economic stability.

In response, the present study aims to assess state-of-the-art cybersecurity strategies for critical infrastructure protection in the era of digitalization. The objective is to systematically map and evaluate these strategies' effectiveness, focusing on their integration into complex, digitized environments and their ability to provide actionable resilience against evolving threats. This research is expected to contribute critical insights for policymakers, infrastructure operators, and security

professionals by identifying best practices, exposing limitations in current approaches, and recommending comprehensive frameworks that advance the security and stability of national critical assets in an increasingly digitalized world. Theoretically, this study extends socio-technical systems theory to the cybersecurity domain by empirically demonstrating how organizational capacity, regulatory clarity, and technological maturity interact to shape defensive effectiveness in critical infrastructure contexts. By documenting the gap between threat sophistication and organizational response capabilities, the research provides a foundation for future theory development regarding adaptive security governance in complex, digitized systems. This theoretical contribution enhances understanding of how institutional factors constrain or enable cybersecurity innovation, offering scholars a framework to examine the organizational determinants of cyber resilience beyond purely technical considerations.

RESEARCH METHOD

This study utilized a descriptive qualitative research design to explore the strategies employed for cybersecurity protection in critical infrastructure during digitalization, involving purposively selected participants such as cybersecurity professionals, IT managers, policymakers, and regulators from key sectors. Data collection was conducted through semi-structured interviews using a validated interview guide focusing on organizational practices, challenges, and innovation adoption, complemented by document analysis of security policies and incident reports, with all instruments pre-tested for validity. Upon obtaining institutional ethics clearance and informed consent, interviews were secured via video conferencing and transcribed for analysis, complying with strict data confidentiality protocols. Thematic analysis was performed on transcripts and documents using both inductive and deductive coding via qualitative analysis software to identify salient patterns and themes, with coding reliability ensured through independent checks and trustworthiness enhanced through member checking and reflexive journaling. All procedures conformed to ethical guidelines, including participant anonymization, secure data handling, and the right to withdraw, underpinning the academic rigor and integrity of the qualitative inquiry.

RESULTS AND DISCUSSION

Threat Landscape and Attack Vectors

The study first explored the types of cyber threats currently facing critical infrastructure organizations. Participants consistently noted that the frequency and sophistication of attacks have risen alongside digitalization initiatives, placing operational environments at heightened risk. A variety of attack vectors were discussed during interviews, ranging from common phishing attempts to complex supply chain intrusions.

Table 1. Reported Frequency of Threat Types Experienced by Critical Infrastructure Organizations

Threat Type	Reported Frequency (%)
Ransomware	63
Phishing	49
Supply Chain Attacks	37
OT-targeted Attacks	22

The data in Table 1 demonstrate that ransomware represents the most prevalent cyber threat, with nearly two-thirds of participants reporting incidents, followed by phishing attacks and supply chain attacks. Operational technology (OT) systems are perceived as increasingly targeted, though reported less frequently, reflecting concerns about their growing exposure during digital transformation efforts.

Organizational Strategies Adopted

Subsequently, the results detail strategic approaches adopted to mitigate identified risks. Participants provided insights into both technical and organizational measures deployed to enhance overall cybersecurity posture, ranging from preventative controls to collaborative efforts with external entities.

Table 2. Adoption Rate of Key Cybersecurity Strategies

Strategy	Adoption (%)
Network Segmentation	56
Employee Training	51
Risk Assessments	46
External Collaboration	38
Real-time Monitoring/Automation	19

As presented in Table 2, network segmentation is the most widely adopted strategy, with employee training also prioritized to enhance organizational resilience. However, advanced solutions like real-time monitoring and automated response remain underutilized, observed in less than one-fifth of organizations. These findings indicate reliance on traditional controls and highlight a lag in adopting dynamic security technologies.

Barriers to Effective Cybersecurity

The research also identified principal barriers that impede robust cybersecurity implementation within critical infrastructure. Participant responses reflected multifaceted challenges, encompassing both structural and operational dimensions.

Table 3. Barriers to Effective Cybersecurity Implementation

Barrier	Reporting (%)
Resource Constraints	67
Regulatory Ambiguity	41
Skills Shortage	40
Legacy System Complexity	35
Incident Coordination Challenges	33

Table 3 reflects that lack of resources emerges as the most frequently cited barrier, affecting more than two-thirds of organizations. Regulatory ambiguity and skills shortages are also prevalent, while integration of legacy systems and difficulties in coordinating incident response further complicate efforts. The cumulative effect of these barriers contributes to ongoing vulnerability in critical sectors.

Table 4. Key Thematic Findings from the Qualitative Analysis

Subtheme	Most Reported Data Point	Reporting (%)
Top Threat	Ransomware	63
Main Strategy	Network Segmentation	56
Primary Barrier	Resource Constraints	67

Table 4 highlights that ransomware, network segmentation, and resource constraints stand out as the most frequently mentioned threat, strategy, and barrier, respectively. These central trends encapsulate the dominant concerns and approaches of professionals currently managing cybersecurity for critical infrastructures.

Ransomware and the Evolving Threat Landscape

The qualitative findings clearly show that ransomware has emerged as the predominant threat to critical infrastructure organizations, echoing recent research that demonstrates its increasing frequency and severity. This escalation is attributed to both technological advancement and the rise of "Ransomware-as-a-Service" (RaaS), which has lowered barriers for cybercriminals and caused significant financial and operational disruptions across sectors such as energy and healthcare. Notably, high-profile cases like the Colonial Pipeline and Universal Health Services ransomware incidents underscore the scale of service paralysis and the ripple effects these attacks produce on public and economic security.

Prior literature corroborates these observations, with multiple studies warning of the compounding risks associated with interconnected operational technologies and the limited visibility these environments often afford defenders. The high rates of reported ransomware within this study align with global analyses that suggest traditional, reactive approaches to cybersecurity are insufficient for the modern era, especially for sectors that underpin societal stability. These findings illuminate the urgency for infrastructure operators to accelerate defensive innovations, augment threat intelligence sharing, and invest in advanced detection and response capacities.

While these insights advance understanding, several limitations are acknowledged, such as reliance on self-reported experiences which may understate actual attack frequencies due to reputational concerns or nondisclosure. Future research should quantify the impact of new mitigation strategies and examine cross-border regulatory approaches for ransomware containment. Further, longitudinal studies tracking the evolution of attack vectors would help assess longer-term effectiveness and resilience of critical infrastructure protections in diverse regulatory contexts.

Organizational Strategies and Capacity Gaps

Findings reveal that many critical infrastructure organizations adopt traditional defensive strategies, such as network segmentation and employee training, but advanced systems like automated real-time monitoring remain poorly adopted. This conservatism reflects prior observations that infrastructure operators often prioritize compliance and baseline controls, postponing more dynamic or resource-intensive measures due to budget or talent shortages. The gap between threat sophistication and strategy adoption heightens vulnerability to evolving cyberattacks.

Existing scholarship stresses the importance of holistic and collaborative security frameworks, emphasizing not only technical defenses but also cross-sector partnerships and regulatory harmonization. The present study reinforces these recommendations: respondents who reported

external collaboration, either with government agencies or industry groups, typically showed higher levels of preparedness and incident response maturity. Accordingly, the findings challenge organizations to go beyond minimum standards, to pursue integrated approaches combining strategic foresight, workforce upskilling, and technology procurement.

Nonetheless, these results are constrained by the qualitative design's focus on selected informants, potentially limiting generalizability. The nature of semi-structured interviews might also bias reporting towards recognized best practices rather than actual everyday practices. Future research could triangulate qualitative insights with quantitative assessments of organizational outcomes, and perform comparative analyses across countries with varying regulatory and cultural environments to determine optimal pathways for capacity building.

Barriers to Implementation and Implications for Policy

Resource constraints, regulatory ambiguity, and legacy system complexity surfaced as major barriers hindering robust cybersecurity implementation, echoing previous analyses which found underfunding, insufficient staffing, and fragmented authority as perennial challenges in the sector. The lack of harmonized regulation is particularly evident in regions where overlapping or unclear mandates produce gaps in responsibility for protection and incident response. This creates an environment where responses to cyber threats are reactive, fragmented, and chronically under-resourced.

Prior studies highlight that organizational and cultural factors are deeply intertwined with technical risk management—as noted in qualitative research linking trust, communication, and leadership values to cybersecurity efficacy. The present study concurs, suggesting that improvements in workforce awareness and the embedding of cybersecurity into daily operational routines may help overcome organizational inertia. From a policy perspective, these findings imply the need for national investments in talent pipelines, incentives for public-private cooperation, and the development of clear, actionable, and enforceable standards for critical infrastructure protection.

Acknowledging study limitations, including a cross-sectional perspective and the absence of sector-wide quantitative benchmarking, further research should examine the effectiveness of new policy interventions in driving security upgrades, especially within under-resourced organizations. Additional scholarship might address the socio-technical dynamics of regulatory coordination and how best to align incentives for wider adoption of best practices across heterogeneous infrastructure sectors.

CONCLUSION

This study set out to assess cybersecurity strategies for the protection of critical infrastructure amid accelerating digitalization, revealing a landscape of persistent and evolving threats—most notably ransomware—while elucidating the defensive strategies, organizational challenges, and systemic barriers shaping current practices. The findings indicate that although organizations have adopted foundational measures such as network segmentation and employee training, substantial gaps remain in the implementation of dynamic defense technologies and resilient incident response, with resource constraints and regulatory ambiguity posing formidable obstacles. Theoretically, the study advances understanding of cybersecurity management in complex infrastructure environments by synthesizing organizational realities with the prevailing threat landscape, providing empirical

evidence that traditional security paradigms are increasingly strained by the scale and sophistication of modern attacks and underscoring the significance of adaptive, collaborative frameworks for sustained protection. Practically, it offers actionable insights for policymakers, regulators, and security professionals, emphasizing targeted investment in technological innovation and workforce development, the cultivation of multi-stakeholder partnerships, and clearer regulatory mandates. Looking ahead, as digitalization deepens, effective protection will hinge on rigorous, evidence-based strategies that bridge the gap between technical capability and organizational capacity; while this research is limited by its qualitative scope and selected sample, future work should employ longitudinal and cross-jurisdictional designs to quantify the impact of advanced defense mechanisms and policy interventions, and address sector-specific and socio-technical complexities to foster adaptive, robust cyber-resilience for the infrastructure foundational to contemporary societies.

REFERENCES

Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information*. https://doi.org/10.3390/INFO15110682

Ahmadi-Assalemi, G., Al-Khateeb, H., Epiphaniou, G., & Maple, C. (2020). Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review. *Smart Cities*. https://doi.org/10.3390/SMARTCITIES3030046

Ajayi, O. O., Alozie, C. E., & Abieba, O. A. (2025). Enhancing Cybersecurity in Energy Infrastructure: Strategies for Safeguarding Critical Systems in the Digital Age. *Trends in Renewable Energy*. https://doi.org/10.17737/TRE.2025.11.2.00192

Ani, U., Watson, J. D. M., Nurse, J. R. C., Cook, A., & Maples, C. D. (2019). A Review of Critical Infrastructure Protection Approaches: Improving Security through Responsiveness to the Dynamic Modelling Landscape. *Living in the Internet of Things (IoT 2019)*. https://doi.org/10.1049/CP.2019.0131

Asiri, M., Saxena, N., Gjomemo, R., & Burnap, P. (2023). Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective. *ACM Transactions on Cyber-Physical Systems*. https://doi.org/10.1145/3587255

Djenna, A., Harous, S., & Saïdouni, D. E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Applied Sciences*. https://doi.org/10.3390/APP11104580

Durojaye, H., & Raji, O. (2022). Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure. *ArXiv*. https://doi.org/10.48550/ARXIV.2212.08036

Jeyaram, A., & Muthukumaravel, A. (2024). Exploring Cyber Threats on Data Engineering Techniques for Identifying Security Breaches. *Advances in Computer and Electrical Engineering Book Series*. https://doi.org/10.4018/979-8-3693-3739-4.CH010

Karabacak, B., Özkan, S., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection*. https://doi.org/10.1016/J.IJCIP.2016.10.001

Kilani, Y. (2020). Cyber-security effect on organizational internal process: mediating role of technological infrastructure. *Problems and Perspectives in Management*. https://doi.org/10.21511/PPM.18(1).2020.39

Ma, H., Lu, Y., Kou, Z., Xue, Z., Yu, W., Zhang, K., Deng, P., Di, C., Zhu, Y., Wang, H., & Chen, Z. (2025). Cybersecurity and Cyber-Attacks in the Growing Natural Gas and Hydrogen Industry: A Systematic Review of Challenges and Opportunities. *Gas Science and Engineering*. https://doi.org/10.1016/J.JGSCE.2025.205744

Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., Benjamin, J., Craig, Benjamin, & Jacob. (2021). Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures. *ArXiv (Cornell University)*. https://doi.org/10.48550/ARXIV.2109.03945

Oroni, C. Z., & Fu, X. (2023). Structural evaluation of management capability and the mediation role of cybersecurity awareness towards enterprise performance. *Journal of Data, Information and Management*. https://doi.org/10.1007/S42488-023-00108-7

Owobu, W. O., Abieba, O. A., Gbenle, P., Onoja, J. P., Daraojimba, A. I., Adepoju, A. H., & Chibunna, U. B. (2022). Conceptual Framework for Deploying Data Loss Prevention and Cloud Access Controls in Multi-Layered Security Environments. *International Journal of Multidisciplinary Research and Growth Evaluation*. https://doi.org/10.54660/.IJMRGE.2022.3.1.850-860

Reddy, K. H. K., Goswami, R. S., & Roy, D. S. (2023). A futuristic green service computing approach for smart city: A fog layered intelligent service management model for smart transport system. *Computer Communications*. https://doi.org/10.1016/J.COMCOM.2023.08.001

Rees, J., & Rees, C. J. (2023). Cyber-Security and the Changing Landscape of Critical National Infrastructure: State and Non-state Cyber-Attacks on Organisations, Systems and Services. *Advanced Sciences and Technologies for Security Applications*. https://doi.org/10.1007/978-3-031-40118-3_5

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Italian National Conference on Sensors*. https://doi.org/10.3390/S23084060

Sulistio. (2023). Assessing the Factors Influencing Cybersecurity Effectiveness: A PLS-SEM Approach. *Information Technologies in Environmental Engineering*. https://doi.org/10.33050/ITEE.V2I1.411

Val, O. O., Kolade, T. M., Gbadebo, M. O., Selesi-Aina, O., Olateju, O. O., & Olaniyi, O. O. (2025). Strengthening Cybersecurity Measures for the Defense of Critical Infrastructure in the United States. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.5021072

Zaydi, M., Maleh, Y., Chênevert, G., Zaydi, H., & Yaagoubi, A. El. (2025). Intelligent Cybersecurity and Resilience for Critical Industries: Challenges and Applications. *River Publishers EBooks*. https://doi.org/10.1201/9788770047746

Zhang, Z., Hamadi, H. Al, Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3204051