IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121048

Enterprise Network Resilience as a National Security Imperative: Strategies for Protecting United States Critical Infrastructure

Temitope Akintunde Ogunwola[1], Fenwa Olusayo Deborah*[2]

Department of Information Technology, University of the Cumberlands, Williamsburg, KY, USA[1]

Department of Computer Science and Engineering, Ladoke Akintola University of Technology, P.M.B 4000, Ogbomoso, Nigeria[2]

*Corresponding Author

Abstract: The security and resilience of enterprise networks in critical infrastructure sectors is a matter of national security, not merely an organizational concern. When ransomware shuts down a hospital network, disrupts power grid control systems, or disables manufacturing automation in defense supply chains, the consequences extend beyond the affected organization to encompass public safety, economic stability, and national security. The United States government has recognized this reality through a series of regulatory and policy actions culminating in the National Security Memorandum on Critical Infrastructure Security and Resilience of April 2024, the Cyber Incident Reporting for Critical Infrastructure Act of 2022, and the National Cybersecurity Strategy of 2023, each of which establishes enterprise network security as a national priority. Yet the gap between national policy aspirations and organizational practice remains significant. This paper synthesizes the enterprise network security and resilience research developed across a five-paper research series addressing software-defined wide area network security, healthcare network compliance, enterprise firewall modernization, acquisition integration security, and critical infrastructure resilience, and presents an integrated strategic framework for enterprise network resilience that aligns practitioner guidance with national security policy requirements. A Three-Pillar Enterprise Network Resilience Framework, organized around architectural hardening, operational continuity, and governance and compliance, provides the synthesis structure. The paper develops a network resilience maturity model that enables critical infrastructure organizations to assess their current resilience posture and identify the specific capability gaps that most directly affect their contribution to national critical infrastructure resilience. The paper contributes a practitioner-validated, policy-aligned framework that connects the technical and operational practices of enterprise network security to the national security goals that those practices serve [31].

Keywords: critical infrastructure resilience, enterprise network security, national security, CIRCIA compliance, NSM-22, network resilience maturity, cybersecurity strategy, zero trust architecture, operational technology security, cyber resilience framework [31].

I. INTRODUCTION

When the Colonial Pipeline ransomware attack of 2021 forced the shutdown of fuel distribution infrastructure serving the eastern United States, it was not a corporate security failure in the ordinary sense of that term. It was a demonstration that enterprise network vulnerabilities in critical infrastructure sectors translate directly into national security consequences. Fuel shortages, panic buying, and emergency declarations across multiple states followed a single ransomware intrusion that exploited network security weaknesses that a more resilient architecture would have contained or prevented. The lesson of Colonial Pipeline, and of the hundreds of similar attacks on healthcare, manufacturing, and communications infrastructure that have followed, is that enterprise network security is a national security issue that demands a framework connecting organizational practice to national policy.

The federal government has responded to this reality with a series of policy actions that collectively establish enterprise network security as a national priority. The National Cybersecurity Strategy of 2023 identified the security of critical infrastructure as a primary national objective and called for the development of sector-specific security frameworks [2]. The National Security Memorandum on Critical Infrastructure Security and Resilience of April 2024 updated the federal framework for critical infrastructure protection, assigned specific security responsibilities to sector risk management agencies, and established enterprise network resilience as a measurable objective for each of the sixteen designated

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121048

critical infrastructure sectors [1]. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 established mandatory incident reporting requirements that create accountability for enterprise network security failures in organizations whose network disruptions affect critical operations [4].

Despite this policy clarity, a significant gap persists between national security policy requirements and the actual network security posture of many critical infrastructure organizations. The average cost of a healthcare data breach reached 10.9 million dollars in 2023 [11], healthcare ransomware incidents more than doubled between 2016 and 2021 [13], and the manufacturing sector continues to account for the highest volume of acquisition-related security incidents [29]. These figures indicate that organizational security practices are not keeping pace with either the threat environment or the policy expectations established by federal frameworks. Closing this gap requires a practitioner-oriented framework that connects the specific technical and operational practices of enterprise network security to the national security goals those practices serve.

Fig. 1 illustrates the relationship between critical infrastructure sectors, the three pillars of enterprise network resilience, and the national security outcomes that resilient enterprise networks support.

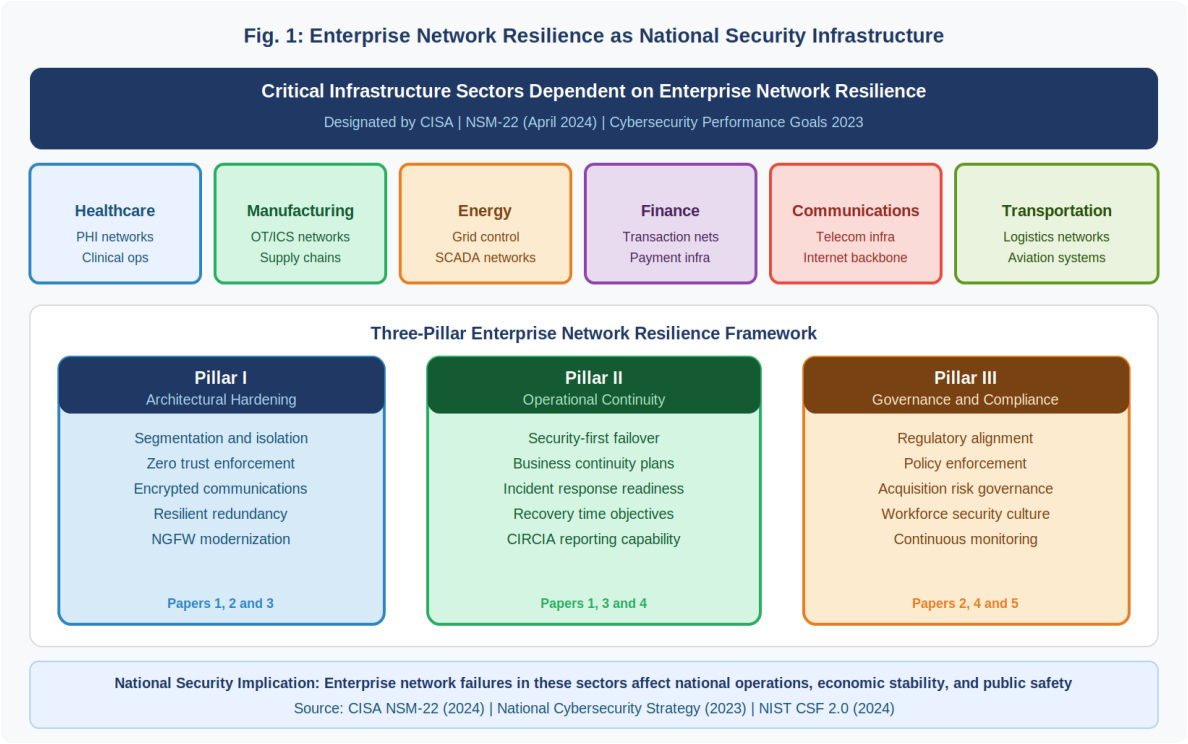

Fig. 1: Enterprise Network Resilience as National Security Infrastructure

Scope and Research Context

This paper serves as the capstone of a five-paper research series examining enterprise network security from multiple perspectives: SD-WAN security and resilience in multi-site enterprise environments; healthcare network security and HIPAA and HITRUST compliance; enterprise firewall modernization for business continuity; cybersecurity and network integration risk management during corporate acquisitions; and the national security implications of enterprise network resilience in critical infrastructure sectors. The scope covers enterprise network security across the sixteen critical infrastructure sectors designated by CISA and updated by NSM-22, drawing on practitioner experience across manufacturing, healthcare, and corporate environments.

Research Objectives and Paper Structure

This paper addresses three research objectives. The first is to characterize the national security significance of enterprise network resilience by connecting organizational network security practices to the national security outcomes they support, using the federal policy framework as the reference for what national security in this domain requires. The second is to develop the Three-Pillar Enterprise Network Resilience Framework, which synthesizes the research contributions of this five-paper series into an integrated strategic framework for enterprise network resilience in critical infrastructure sectors. The third is to present a network resilience maturity model that enables critical infrastructure

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121048

organizations to assess their current resilience posture against national policy expectations and identify the capability gaps that most directly affect their contribution to national critical infrastructure resilience.

This paper proceeds as follows. Section II reviews the national policy and regulatory framework for enterprise network resilience. Section III presents the threat landscape facing enterprise networks in critical infrastructure sectors. Section IV develops the Three-Pillar Enterprise Network Resilience Framework. Section V presents the network resilience maturity model. Section VI discusses implementation experience and findings. Section VII concludes with contributions and future research directions.

II. NATIONAL POLICY AND REGULATORY FRAMEWORK

A. The Evolution of Federal Critical Infrastructure Cybersecurity Policy

Federal policy governing critical infrastructure cybersecurity has evolved substantially since the original Presidential Policy Directive 21 of 2013, moving from a general framework for public-private partnership to a more specific and accountability-oriented set of requirements. NSM-22 of April 2024 replaced PPD-21 and reflected a significantly changed strategic environment characterized by more sophisticated adversaries, greater dependence on networked critical infrastructure, and accumulated evidence that voluntary cybersecurity improvement had not produced the sector-wide resilience improvements that previous policy approaches anticipated [1]. NSM-22 assigned specific responsibilities to sector risk management agencies, established requirements for sector risk assessments and risk management plans and directed the National Coordinator for Critical Infrastructure Security and Resilience to coordinate cross-sector risk identification and analysis.

The National Cybersecurity Strategy Implementation Plan of July 2023 provided specific actions and timelines for implementing the strategy's objectives, identifying enterprise network security in critical sectors as a priority area for framework development and federal assistance [3]. Together, these three policy documents establish a coherent national framework that defines what enterprise network resilience in critical infrastructure sectors should look like and what the federal government expects of organizations in those sectors.

B. CIRCIA and Mandatory Incident Reporting

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 represents the most significant expansion of federal authority over critical infrastructure cybersecurity since the establishment of CISA in 2018. CIRCIA requires covered entities in critical infrastructure sectors to report substantial cyber incidents to CISA within 72 hours of the time the entity reasonably believes a covered incident has occurred, and to report ransomware payments within 24 hours [4]. The proposed rulemaking published by CISA in April 2024 estimated that more than 300,000 entities would be covered by the regulation, reflecting the broad scope of what CISA considers critical infrastructure.

For enterprise network security practitioners, CIRCIA has direct implications for network architecture, monitoring capabilities, and incident response planning. Organizations must maintain detection capabilities sufficient to identify covered incidents within timeframes that enable the required reporting. They must maintain network monitoring and logging infrastructure that can support the incident characterization information required by CIRCIA reports. And they must have incident response plans that include CIRCIA reporting procedures and that are tested under conditions that reflect the types of incidents most likely to require reporting.

The CIRCIA reporting requirements also have implications for organizations managing network changes through acquisitions, system upgrades, and infrastructure modernization. During these transition periods, detection coverage gaps are most likely to exist, and the organizational complexity of major infrastructure changes creates conditions in which CIRCIA reporting obligations may not be clearly assigned or understood by all relevant personnel. The acquisition integration security framework developed in Paper 4 specifically addresses CIRCIA compliance continuity through acquisition-related network changes.

C. NIST Frameworks and Standards

The CISA Cybersecurity Performance Goals, published in 2023, translate the broad requirements of NIST frameworks into specific, measurable actions that critical infrastructure entities can implement to meaningfully reduce their risk [14]. The CPGs represent a minimum baseline of network security practices that CISA considers necessary for critical infrastructure organizations, and they provide a concrete reference point for the network resilience maturity model presented in Section V.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121048

III. THREAT LANDSCAPE AND RESILIENCE IMPERATIVES

A. The Threat Environment Facing Critical Infrastructure Networks

The threat landscape facing enterprise networks in critical infrastructure sectors has intensified in each of the years examined by this research series. The IBM Security X-Force Threat Intelligence Index 2024 identified manufacturing as the most targeted industry for the third consecutive year, with ransomware and data theft as the dominant attack objectives [12]. Healthcare, which is the focus of the compliance framework developed in Paper 2, experienced 742 significant data breaches in 2023, with hacking and IT incidents accounting for 77 percent of all reported breaches [13]. The ENISA Threat Landscape 2023 identified ransomware, data-related threats, and distributed denial of service attacks as the three most significant threat categories for critical infrastructure, with nation-state actors increasingly targeting critical infrastructure as a component of geopolitical competition [20].

Fig. 2 presents the threat landscape facing enterprise network infrastructure in critical infrastructure sectors alongside the specific resilience countermeasures that address each threat category.

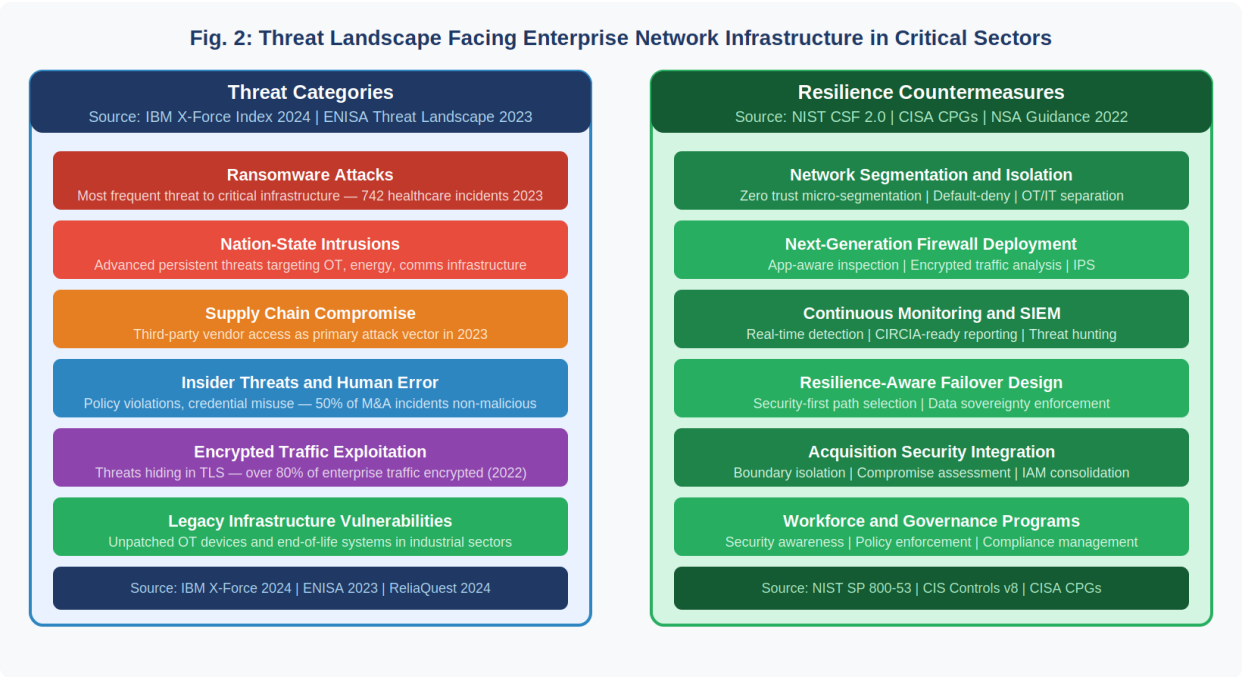

Fig. 2: Threat Landscape Facing Enterprise Network Infrastructure in Critical Sectors

The cyber resilience research conducted by Alablani and Alenazi on industrial networks documented the specific characteristics of cyberattack impacts on operational technology environments, finding that attacks on industrial control systems and industrial IoT create disproportionate operational disruptions relative to equivalent attacks on information technology networks [10]. This finding supports the research program's emphasis on OT-specific security practices in both the SD-WAN security framework of Paper 1 and the acquisition integration framework of Paper 4, where OT network isolation and latency-sensitive security controls are specifically addressed.

B. The Resilience Gap in Critical Infrastructure Organizations

Despite the availability of comprehensive security frameworks, federal guidance, and significant federal assistance, a substantial gap persists between required and actual security postures across critical infrastructure sectors. The IBM Cost of a Data Breach Report 2023 found that healthcare had the highest average breach cost of any industry at 10.9 million dollars, a figure that has increased consistently for more than a decade despite comprehensive HIPAA and HITRUST regulatory frameworks [11]. In manufacturing, ReliaQuest's 2024 analysis found that 42 percent of M&A-related cybersecurity incidents occurred in manufacturing organizations, with legacy OT systems and inadequate network segmentation as the primary vulnerability factors [29]. These findings are consistent across the research program and point to network segmentation inadequacy and legacy infrastructure as the primary drivers of poor security outcomes.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121048

IV. THREE-PILLAR ENTERPRISE NETWORK RESILIENCE FRAMEWORK

The Three-Pillar Enterprise Network Resilience Framework synthesizes the research contributions of this five-paper series into an integrated strategic framework for enterprise network resilience in critical infrastructure sectors, organized around three pillars: architectural hardening, operational continuity, and governance and compliance. Fig. 3 illustrates the policy and regulatory framework the three pillars are designed to satisfy, the enterprise implementation layer organized around those pillars, and the national security outcomes that effective implementation supports.
Table I maps the ten primary enterprise network resilience dimensions to specific practices, governing authorities, and research contributions across the five-paper series.

TABLE I ENTERPRISE NETWORK RESILIENCE DIMENSIONS: PRACTICES, AUTHORITIES, AND RESEARCH CONTRIBUTIONS

Resilience Dimension	Enterprise Practice	Governing Authority	Research Paper
Architecture Hardening	Zero trust SD-WAN security framework	NIST CSF 2.0 / NSA Guidance	Paper 1
Regulatory Compliance	HIPAA and HITRUST healthcare network security	HHS / HITRUST Alliance	Paper 2
Infrastructure Modernization	NGFW migration for business continuity	CISA CPGs / Gartner	Paper 3
Acquisition Governance	Four-stage acquisition network integration	CIRCIA 2022 / NIST SP 800-37	Paper 4
National Security Posture	Cross-sector resilience strategy synthesis	NSM-22 / National Cyber Strategy	Paper 5
Incident Reporting	CIRCIA coverage across all enterprise systems	CISA CIRCIA 2022	Papers 4 and 5
OT/ICS Protection	Industrial network isolation and monitoring	NSA Guidance / NIST SP 800-160	Papers 1, 3 and 4
Zero Trust Enforcement	Micro-segmentation and identity verification	NIST SP 800-207 / CISA ZTMM	Papers 1, 2 and 4
Continuous Monitoring	SIEM integration and threat detection	NIST SP 800-53 / CIS Controls	Papers 1, 2, 3 and 5
Workforce Governance	Security culture and policy enforcement	CISA CPGs / NIST CSF Govern	Papers 2, 4 and 5

A. Pillar I: Architectural Hardening

Architectural hardening encompasses the technical design decisions that determine an organization's attack surface, its ability to contain network intrusions, and its capacity to protect sensitive data in transit and at rest. The research contributions of Papers 1, 2, and 3 each address specific dimensions of architectural hardening: SD-WAN security architecture and zero trust network segmentation, healthcare network compliance architecture and medical device isolation, and enterprise firewall modernization for next-generation threat prevention.

The zero trust principle that no network communication should be implicitly trusted, regardless of its origin, is the architectural foundation that underlies all three papers' specific recommendations. Implementing zero trust in practice requires micro-segmentation that places all network resources in segments with explicit access controls, network monitoring that provides visibility into all inter-segment communication, and identity-aware policy enforcement that restricts access based on verified user and device identity rather than network location. The convergence of CISA's Zero Trust Maturity Model guidance and NIST Special Publication 800-207 on this architectural approach establishes zero trust network segmentation as the primary technical control for architectural hardening in critical infrastructure networks [16][17].

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121048

Firewall modernization, addressed specifically in Paper 3, is the prerequisite technology investment that enables zero trust architecture at the network layer. Organizations operating legacy stateful packet inspection firewalls that cannot perform application identification, user identity enforcement, or encrypted traffic inspection cannot implement the architectural controls required by federal frameworks or by the threat environment their networks face. The phased migration approach developed in Paper 3 provides a business continuity framework for making this fundamental infrastructure transition without disrupting the operations that critical infrastructure networks support.

B. Pillar II: Operational Continuity

Operational continuity addresses the security practices that ensure critical infrastructure networks remain functional and secure during operational challenges including cyberattacks, natural disasters, equipment failures, and the organizational changes that result from growth, acquisitions, and infrastructure modernization. Papers 1 and 3 each address specific dimensions of operational continuity: resilience-aware failover design that maintains security policy continuity when primary network paths fail, and business continuity provisions for firewall migration that ensure security coverage is maintained throughout major infrastructure transitions.

CIRCIA compliance is a central operational continuity requirement for organizations in critical infrastructure sectors. Maintaining the detection and reporting capabilities required by CIRCIA through acquisitions, infrastructure changes, and network architecture evolution is an operational challenge that requires dedicated planning and governance. Organizations that experience covered cyber incidents but cannot report them within the required 72-hour window because their detection systems have coverage gaps or their incident response procedures have not been updated to reflect current network architecture create regulatory exposure that compounds the operational damage of the underlying incident.

The cyber resilience engineering framework of NIST SP 800-160 Volume 2 provides the engineering foundation for operational continuity in critical infrastructure networks [6]. Its four cyber resiliency goals of anticipating, withstand, recovering, and adapting define the capability dimensions that operationally resilient networks must demonstrate, and map directly to the specific operational continuity practices addressed across this research program.

C. Pillar III: Governance and Compliance

Governance and compliance address the organizational structures, policies, processes, and accountability mechanisms that sustain architectural hardening and operational continuity over time. Technical security controls cannot maintain their effectiveness without organizational governance processes that enforce policy compliance, manage security program evolution, and ensure that security requirements are reflected in organizational decision-making including acquisition planning, infrastructure investment, and workforce development.

The NSM-22 of April 2024 specifically addressed governance at the national level, establishing roles and responsibilities for sector risk management agencies, creating accountability for cross-sector risk identification, and directing the development of sector-specific risk management plans [1]. At the organizational level, governance requirements flow from multiple sources: CIRCIA's mandatory reporting requirements create accountability for incident detection and response capabilities; CISA's Cybersecurity Performance Goals establish minimum baseline security practices for critical infrastructure entities [14]; and sector-specific regulations such as HIPAA for healthcare establish compliance frameworks that governance structures must satisfy.

Acquisition security governance, addressed specifically in Paper 4, is a governance dimension that has received insufficient attention in existing frameworks. Organizations that acquire other entities in critical infrastructure sectors face governance challenges that extend well beyond the technical integration of network systems, requiring governance processes that maintain CIRCIA compliance continuity, preserve regulatory status through organizational transitions, and integrate acquired organizations into existing security governance structures without creating compliance gaps or security control vacancies.

V. ENTERPRISE NETWORK RESILIENCE MATURITY MODEL

The Enterprise Network Resilience Maturity Model provides critical infrastructure organizations with a structured framework for assessing their current resilience posture and identifying the capability gaps that most directly affect their contribution to national critical infrastructure resilience. The model defines five maturity levels that represent a progression from initial security postures characterized by fundamental vulnerabilities to optimizing postures characterized by adaptive, intelligence-driven security capabilities.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121048

Fig. 5 illustrates the five-level maturity model, with associated security characteristics at each level and an indication of the overall risk posture associated with each level.

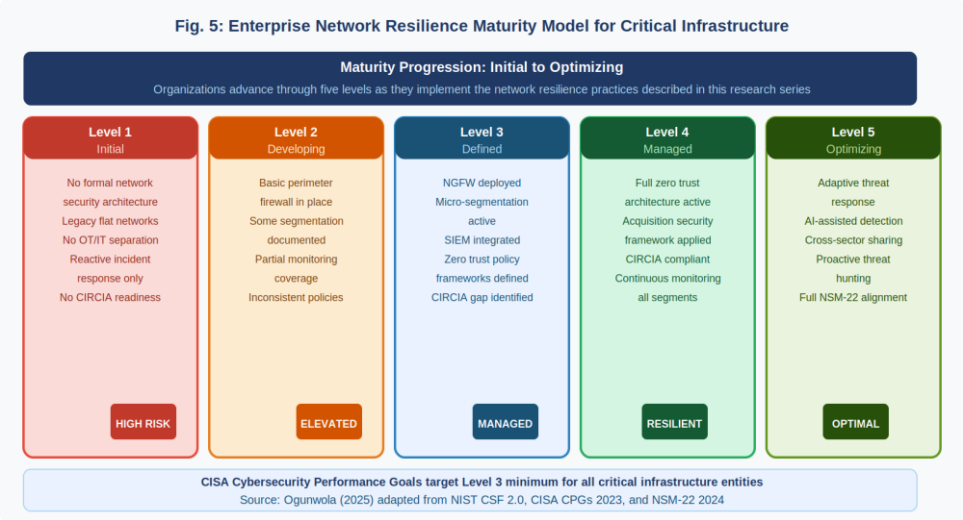

Fig. 5: Enterprise Network Resilience Maturity Model for Critical Infrastructure

The CISA Cybersecurity Performance Goals establish Level 3 as the minimum acceptable maturity level for critical infrastructure entities [14]. At Level 3, organizations have deployed next-generation firewall infrastructure, implemented micro-segmentation, integrated SIEM monitoring, defined zero trust policy frameworks, and identified their CIRCIA compliance gaps. Organizations below Level 3 represent an elevated risk to both their own operations and to the critical infrastructure sectors they serve. The model is designed to be self-assessable against the specific practices and capabilities described across the five-paper research series, with each pillar and maturity level mapping directly to published federal standards.

VI. IMPLEMENTATION EXPERIENCE AND POLICY IMPLICATIONS

A. Cross-Sector Implementation Findings

The implementation experience accumulated across the five-paper research series provides a cross-sector view of how the three pillars of enterprise network resilience translate into operational practice in healthcare, manufacturing, and corporate network environments. Several findings are consistent across sectors and warrant particular emphasis for their policy implications.

Network segmentation implementation consistently reveals network architecture characteristics that are not apparent from documentation review alone. Clinical data flow mapping in healthcare environments regularly surfaces undocumented applications transmitting protected health information over unencrypted paths. Pre-acquisition network assessments in manufacturing environments identify OT devices connected to corporate networks without appropriate isolation. Post-merger network analysis in corporate environments uncovers legacy systems with security configurations that were never designed to meet contemporary security standards. The consistency of these findings across sectors suggests that documentation-based compliance assessments systematically underestimate the actual security posture of critical infrastructure organizations.

The gap between documented security policy and implemented security controls is the most important operational finding of this research series. Organizations in every sector examined have written security policies that are more stringent than their implemented technical controls. Firewall rule bases contain policies that are no longer enforced or that contradict the organization's stated security architecture. Network monitoring systems have coverage gaps that leave significant portions of the network environment unobserved. Identity management systems contain accounts with privileges that exceed documented access control policies. These gaps between documented policy and implemented controls are the primary vulnerability pathway exploited by ransomware and other attacks on critical infrastructure organizations.

B. CIRCIA Implementation Readiness Across Sectors

The CIRCIA compliance implications of the network security practices developed across this research series deserve specific attention as final CIRCIA rulemaking approaches. Organizations that have implemented the architectural

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121048

hardening practices of Pillar I are significantly better positioned for CIRCIA compliance than those that have not, because zero trust micro-segmentation and SIEM integration provide the detection capabilities that CIRCIA reporting requires. Organizations operating flat networks with limited monitoring coverage will find CIRCIA compliance operationally challenging because they cannot reliably detect covered incidents within the timeframes that CIRCIA requires.

The acquisition integration challenge for CIRCIA compliance identified in Paper 4 is particularly acute for organizations in active growth-by-acquisition mode. Each acquisition creates a period during which detection coverage is uncertain, organizational responsibility for CIRCIA reporting may not be clearly assigned in the acquired entity, and the 72-hour reporting window may be impossible to meet for incidents originating in newly integrated systems. Organizations that have implemented the Four-Stage Acquisition Network Integration Security Framework developed in Paper 4 are specifically designed to maintain CIRCIA compliance continuity through acquisition integration, but organizations without such a framework face a genuine regulatory risk during each integration period.

C. National Security Policy Recommendations

The research findings across this series support several recommendations for national cybersecurity policy that would improve the effectiveness of existing frameworks in driving enterprise network resilience in critical infrastructure sectors.

First, federal sector risk management agencies should develop sector-specific guidance that translates the general network security requirements of NSM-22 and CISA CPGs into architecture-level specifications for their sectors. The general requirements of frameworks like the NIST CSF leave too much implementation discretion to organizations, many of which lack the technical expertise to translate high-level framework requirements into specific network architecture decisions. Healthcare organizations implementing Paper 2's Five-Component Healthcare Network Compliance Framework benefit from sector-specific guidance that connects HIPAA Technical Safeguards to specific network design decisions; equivalent guidance should exist for each critical infrastructure sector.

Second, CIRCIA implementation should include technical assistance for critical infrastructure organizations that need to upgrade their detection capabilities to meet the 72-hour reporting requirement. The practical challenge of CIRCIA compliance is not primarily organizational; it is technical. Organizations without adequate network monitoring infrastructure cannot detect covered incidents within CIRCIA's reporting timeframes regardless of their organizational commitment to compliance. Federal technical assistance for network monitoring infrastructure investment in critical infrastructure organizations would directly address this gap.

Third, acquisition security governance should be specifically addressed in sector risk management plans and in CIRCIA implementation guidance. The acquisition integration period is one of the highest-risk periods for critical infrastructure organizations, and existing frameworks do not adequately address the specific security challenges that acquisitions create. The Four-Stage Acquisition Network Integration Security Framework developed in Paper 4 provides a model that federal guidance could adapt for sector-specific implementation.

D. Quantitative Indicators of the Resilience Gap

The scale of the enterprise network resilience gap in critical infrastructure sectors is measurable through several key data points drawn from the verified sources underpinning this research series. In healthcare, ransomware attacks on hospitals and health systems more than doubled between 2016 and 2021, exposing the protected health information of nearly 42 million patients over that period [13]. The average cost of a healthcare data breach reached 10.9 million dollars in 2023, the highest of any industry sector and more than double the cross-industry average [11]. These figures represent organizations that are regulated by HIPAA, subject to HITRUST assessment, and covered by the compliance framework developed in Paper 2 of this series yet continue to experience breach rates and costs that have increased year over year.

In manufacturing, ReliaQuest's 2024 analysis found that manufacturing accounted for 42 percent of all acquisition-related security incidents, with legacy operational technology systems and inadequate network segmentation identified as the primary contributing factors [29]. The IBM X-Force Threat Intelligence Index 2024 identified manufacturing as the most targeted industry for the third consecutive year, with ransomware and data theft representing the dominant attack objectives [12]. These figures are consistent with the findings of the industrial network cyber resilience research of Alablani and Alenazi, who documented the disproportionate operational impact of cyberattacks on industrial control system environments relative to equivalent attacks on information technology networks [10].

Across all critical infrastructure sectors, the CISA 2024 Year in Review reported continued increases in the frequency and severity of cyber incidents affecting critical infrastructure, with ransomware remaining the most disruptive attack category for operational continuity [5]. CISA estimates that more than 300,000 entities will be covered by the final

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 10, October 2025

DOI: 10.17148/IARJSET.2025.121048

CIRCIA regulations [4], of which only a fraction currently have the network monitoring and detection capabilities required to meet the 72-hour incident reporting requirement. The gap between the number of organizations subject to CIRCIA and the number with adequate detection infrastructure represents the most concrete and measurable dimension of the enterprise network resilience deficit that this research series addresses.

CONCLUSION

This paper has developed the Three-Pillar Enterprise Network Resilience Framework, synthesizing the research contributions of a five-paper series into an integrated strategic framework that connects enterprise network security practices to national security policy requirements. The framework's three pillars of architectural hardening, operational continuity, and governance and compliance provide a structured approach to enterprise network resilience that addresses the technical, operational, and organizational dimensions of security in critical infrastructure sectors.

The research makes four contributions. It provides the first integrated framework connecting enterprise network security practices across multiple domains, specifically SD-WAN security, healthcare network compliance, firewall modernization, acquisition security, and critical infrastructure resilience, into a unified strategic framework aligned with national security policy. It develops a network resilience maturity model that enables critical infrastructure organizations to assess their posture against the CISA Cybersecurity Performance Goals and NIST CSF 2.0 requirements. It identifies the CIRCIA compliance implications of enterprise network architecture choices, acquisition integration practices, and monitoring capability gaps, providing practitioners with actionable guidance for maintaining regulatory compliance through organizational and infrastructure changes. It connects organizational network security practices to national security outcomes in terms that support both practitioner decision-making and policy development.

The national security significance of enterprise network resilience will only increase as critical infrastructure sectors continue to digitize operations, connect previously isolated systems, and expand network-dependent services. Organizations that treat network security as a technical operational concern rather than a national security obligation are both underestimating the stakes of their security decisions and missing the opportunity to contribute to the resilience of the critical systems on which national security depends. The frameworks, practices, and policy connections developed in this research series are intended to help close that gap.

Future research should examine the quantitative relationship between specific network security maturity levels and critical infrastructure disruption outcomes, providing empirical evidence base for cost-benefit analyses of security investment on a national scale. The adaptation of these frameworks to the emerging operational technology security requirements of smart grid, connected transportation, and next-generation industrial systems represents a priority research direction as these sectors undergo rapid digitization. And longitudinal study of CIRCIA compliance rates and outcomes across sectors will provide important evidence about the effectiveness of mandatory incident reporting as a tool for improving national critical infrastructure resilience.

ACKNOWLEDGMENT

The author acknowledges the contributions of the network security, critical infrastructure protection, and cybersecurity policy communities whose scholarship and operational experience informed this research series, and the academic support of the Department of Information Technology at the University of the Cumberlands.

REFERENCES

[1] The White House National Security Council, “National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22),” The White House, Washington, D.C., April 2024. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

[2] The White House, “National Cybersecurity Strategy,” Executive Office of the President, Washington, D.C., March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[3] The White House, “National Cybersecurity Strategy Implementation Plan,” Executive Office of the President, Washington, D.C., July 2023. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf

[4] Cybersecurity and Infrastructure Security Agency, “Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),” CISA, Washington, D.C., 2022. https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-for-critical-infrastructure-act-2022-circia

DOI: 10.17148/IARJSET.2025.121048

[5] Cybersecurity and Infrastructure Security Agency, "2024 Year in Review: CISA's Achievements in Reducing Risk and Building Resilience," CISA, Washington, D.C., 2024. https://www.cisa.gov/news-events/news/2024-year-review-highlights-cisas-achievements-reducing-risk-and-building-resilience-cybersecurity

[6] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau and R. McQuaid, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," NIST Special Publication 800-160 Vol. 2 Rev. 1, National Institute of Standards and Technology, Gaithersburg, MD, 2022. https://doi.org/10.6028/NIST.SP.800-160v2r1

[7] National Institute of Standards and Technology, "The NIST Cybersecurity Framework 2.0," NIST, Gaithersburg, MD, 2024. https://doi.org/10.6028/NIST.CSWP.29

[8] R. Ross, V. Pillitteri, K. Graubart, D. Bodeau and R. McQuaid, "Engineering Trustworthy Secure Systems," NIST Special Publication 800-160 Vol. 1 Rev. 1, National Institute of Standards and Technology, Gaithersburg, MD, 2022. C

[9] Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," CISA, Washington, D.C., 2023. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[10] I. Alablani and M. Alenazi, "Cyber Resilience in Industrial Networks: A State of the Art, Challenges, and Future Directions," Journal of King Saud University: Computer and Information Sciences, vol. 35, no. 9, pp. 101781, 2023. https://doi.org/10.1016/j.jksuci.2023.101781

[11] C. Liu and M. A. Babar, "Corporate Cybersecurity Risk and Data Breaches: A Systematic Review of Empirical Research," Australian Journal of Management, 2024. https://doi.org/10.1177/03128962241293658

[12] IBM Security, "X-Force Threat Intelligence Index 2024," IBM Corporation, Armonk, NY, 2024. https://www.ibm.com/reports/threat-intelligence

[13] H. T. Neprash, C. C. McGlave, D. A. Cross, B. A. Virnig, M. A. Puskarich, A. Huling, A. Rozenshtein and S. S. Nikpay, "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021," JAMA Health Forum, vol. 3, no. 12, e224873, 2022. https://doi.org/10.1001/jamahealthforum.2022.4873

[14] Cybersecurity and Infrastructure Security Agency, "Cross-Sector Cybersecurity Performance Goals," CISA, Washington, D.C., 2023. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[15] U.S. Department of Health and Human Services, "Healthcare and Public Health Sector: Cybersecurity Performance Goals," HHS, Washington, D.C., 2023. https://aspr.hhs.gov/cyber/Documents/Healthcare-CPGs-508.pdf

[16] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model, Version 2.0," CISA, Washington, D.C., 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[17] S. Rose, O. Borchert, S. Mitchell and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, 2020. https://doi.org/10.6028/NIST.SP.800-207

[18] National Security Agency, "Network Infrastructure Security Guidance," NSA Cybersecurity Technical Report, National Security Agency, Fort Meade, MD, 2022. https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDANCE_20220615.PDF

[19] S. Kaur, M. Syed and J. Rana, "Towards a Framework for Improving Cyber Security Resilience of Critical Infrastructure Against Cyber Threats: A Dynamic Capabilities Approach," Technology Analysis and Strategic Management, 2025. https://doi.org/10.1080/09537325.2025.2479546

[20] European Union Agency for Cybersecurity, "ENISA Threat Landscape 2023," ENISA, Athens, Greece, 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[21] ISO/IEC, "Information Security Management Systems: Requirements," ISO/IEC 27001:2022, International Organization for Standardization, Geneva, Switzerland, 2022. https://www.iso.org/standard/82875.html

[22] Center for Internet Security, "CIS Critical Security Controls Version 8," CIS, East Greenbush, NY, 2021. https://www.cisecurity.org/controls/v8

[23] R. Ross, V. Pillitteri, K. Dempsey and M. Riddle, "Security and Privacy Controls for Information Systems and Organizations," NIST Special Publication 800-53 Rev. 5, NIST, Gaithersburg, MD, 2022. https://doi.org/10.6028/NIST.SP.800-53r5

[24] B. A. A. Nunes, M. Mendonca, X. Nguyen, K. Obraczka and T. Turletti, "Software-Defined Wide Area Networks: Current Challenges and Future Perspectives," in Proc. IEEE Int. Conf. Communications, 2023. https://doi.org/10.1109/ICC45041.2023.10175458

[25] Y. He, D. Huang, L. Chen, Y. Ni and X. Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends," Wireless Communications and Mobile Computing, vol. 2022, pp. 1-13, 2022. https://doi.org/10.1155/2022/6476274

[26] U.S. Department of Health and Human Services, "HIPAA Security Rule: Summary and Guidance for Implementation," HHS Office for Civil Rights, Washington, D.C., 2022. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

DOI: 10.17148/IARJSET.2025.121048

[27] A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap and K. Salonitis, "Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations," Sensors, vol. 23, no. 9, p. 4539, 2023. https://doi.org/10.3390/s23094539

[28] M. Rahouti, K. Xiong and N. Ghani, "SDN Security Review: Threat Taxonomy, Implications, and Open Challenges," IEEE Access, vol. 10, pp. 45820-45854, 2022. https://doi.org/10.1109/ACCESS.2022.3165096

[29] G. T. M. Vu, K. Hoang and H. V. Hoang, "Merger and Acquisition, Firm-Level Cybersecurity Risk, and Research and Development Intensity," Managerial and Decision Economics, vol. 45, no. 5, pp. 3094-3106, 2024. https://doi.org/10.1002/mde.4190

[30] Cybersecurity and Infrastructure Security Agency, "Cybersecurity Performance Goals: Sector-Specific and Cross-Sector Goals for Critical Infrastructure," CISA, Washington, D.C., 2023. https://www.cisa.gov/cybersecurity-performance-goals-cpgs

[31] T. A. Ogunwola, "Security and Resilience Considerations for Software-Defined Wide Area Network Deployments in Multi-Site Enterprise Environments," International Advanced Research Journal in Science, Engineering and Technology (IARJSET), 2025. https://doi.org/10.17148/IARJSET.2025.12150

BIOGRAPHY

Temitope Akintunde Ogunwola is a doctoral candidate in Information Technology at the University of the Cumberlands, Williamsburg, Kentucky, with research focused on enterprise cybersecurity, network security infrastructure, and the intersection of organizational security practice with national security policy. He has over 16 years of professional experience in network security and IT infrastructure management across manufacturing, healthcare, and corporate environments. He currently serves as Staff Network Engineer at Watkins Wellness. Certifications include CISM, CISA, CCNP, CCNP Security, and PCNSE. This paper is the fifth in a five-paper research series on enterprise network security and critical infrastructure resilience.

Fenwa Olusayo Deborah is a faculty member in the Department of Computer Science and Engineering at Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria. Her research interests include network security, critical infrastructure protection, cybersecurity governance, and information systems. She is the corresponding author for this paper.