Scientific Research Publishing

Journal of Software Engineering and Applications, 2026, 19(5), 171-203
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

A Conceptual Framework to Illustrate Cybersecurity Workforce Gaps and the Resilience of Critical Digital Infrastructure—A Multi-Sector Case Study

Samuel-Noah Osarenkhoe[1*], Aihie Osarenkhoe[2#]

[1]Global Partners LP, Waltham, MA, USA
[2]Department of Business & Economic Studies, University of Gävle, Gävle, Sweden
Email: sosarenkhoe@outlook.com, [#]aihie.osarenkhoe@hig.se

How to cite this paper: Osarenkhoe, S.-N. and Osarenkhoe, A. (2026) A Conceptual Framework to Illustrate Cybersecurity Workforce Gaps and the Resilience of Critical Digital Infrastructure—A Multi-Sector Case Study. *Journal of Software Engineering and Applications*, **19**, 171-203.
https://doi.org/10.4236/jsea.2026.195009

Received: March 21, 2026
Accepted: May 3, 2026
Published: May 6, 2026

Abstract

This study examines how cybersecurity workforce shortages undermine the resilience of critical digital infrastructure, with emphasis on the energy sector and comparisons to finance, transportation, and telecommunications. It reframes the skills gap as a systemic risk that weakens organizations' capacity to prevent, manage, and recover from cyber incidents. Using a two-phase qualitative approach—a PRISMA-guided literature review (n = 70) and multi-sector case studies (n = 5) based on 22 interviews—the analysis draws on socio-technical systems theory. Findings show that resilience is limited less by missing technical controls than by a lack of hybrid professionals who can bridge Information Technology (IT), Operational Technology (OT) and Artificial Intelligence domains. Shortages slow incident response, impede risk communication, and reduce coordination. The study concludes that workforce capability is central to infrastructure resilience, requiring sector-aligned training, interdisciplinary collaboration, and continuous upskilling. Policy measures should support cross-sector training and educational reform. Limitations include the small qualitative sample, suggesting future global and AI-human studies.

Keywords

Cybersecurity Workforce Shortage, Critical Infrastructure Resilience, Socio-Technical Systems, Operational Technology, Hybrid-Skilled Professionals, PRISMA Systematic Literature Review, Multi-Sector Case Study

*Main/first author.
[#]Corresponding author.

1. Introduction and Background to the Research Problem

The accelerating digitization of critical infrastructure sectors—including energy, finance, transportation, and telecommunications—has intensified reliance on complex, interconnected cyber-physical systems [1]-[3]. While this transformation enhances operational efficiency and system integration, it simultaneously expands the cyber threat landscape, exposing essential services to risks that extend beyond technical disruption to include national security, economic stability, and public trust [4]-[6].

In this evolving context, cybersecurity challenges are increasingly understood as socio-technical in nature, arising from the interaction of people, technologies, organizational processes, and regulatory environments [7] [8]. The convergence of Information Technology (IT), Operational Technology (OT), and emerging domains such as Artificial Intelligence (AI) has further intensified system complexity, requiring coordinated expertise that spans technical, operational, and strategic domains [3] [9] [10]. As a result, cybersecurity effectiveness is no longer determined solely by technological sophistication, but by the capacity of organizations to align human and technical components within complex operational settings.

A persistent and critical constraint across these sectors is the global shortage of cybersecurity professionals. Although demand for cybersecurity expertise continues to grow, the available workforce remains insufficient in both scale and capability [11] [12]. Importantly, this shortage reflects not only a numerical deficit but also a qualitative gap in hybrid-skilled professionals capable of bridging IT, OT, AI, and organizational functions [13] [14]. Without such integrative expertise, even well-designed cybersecurity frameworks and advanced tools cannot be effectively operationalized in real-world environments [4] [15].

The implications of this workforce gap are particularly pronounced in the energy sector, where legacy operational technologies, safety-critical processes, and strict regulatory environments create uniquely complex cybersecurity challenges [3] [16]. In such contexts, cybersecurity decisions must balance risk mitigation with the continuity of essential services, such as electricity and fuel supply. However, similar workforce-related constraints—such as delayed incident response, coordination failures, and skill mismatches—have also been observed in other critical sectors, including transportation [6], finance [5], healthcare [17], and telecommunications [18]. These recurring patterns suggest that workforce capability may represent a systemic determinant of resilience across sectors, rather than a context-specific issue.

Despite growing awareness of cybersecurity workforce shortages, existing research has largely focused on technical controls, policy frameworks, or generalized workforce metrics [1] [2] [14]. There remains limited empirical understanding of how workforce capability shapes the operational resilience of cybersecurity practices, particularly in high-risk, regulated environments such as energy. Furthermore, cross-sector comparative research remains underdeveloped, leaving

unclear which workforce-related challenges are systemic and which are shaped by sector-specific socio-technical conditions.

To address this gap, this study adopts a Socio-Technical Systems (STS) perspective [7] [19] and employs a multi-method qualitative design combining a PRISMA-guided systematic literature review with empirical case studies across the energy, transportation, finance, and telecommunications sectors. While maintaining a primary analytical focus on the energy sector, the inclusion of non-energy cases serves a deliberate comparative purpose. These cases function as analytical contrasts and parallels, enabling the identification of recurring cross-sector mechanisms—such as hybrid skill shortages, coordination breakdowns, and delayed incident response—while clarifying how the energy sector's distinctive characteristics amplify or reshape these dynamics.

Through this comparative approach, the study reframes the cybersecurity workforce gap not merely as a staffing issue, but as a systemic socio-technical constraint on infrastructure resilience, affecting how organizations anticipate, manage, and recover from cyber incidents across critical sectors.

Research Question

In response to the identified research gap, this study is guided by the following overarching research question:

RQ: How do cybersecurity workforce shortages affect the resilience of critical digital infrastructure across sectors, and how are these effects shaped by the socio-technical characteristics of the energy sector?

This question reflects the need to understand cybersecurity workforce capability as a systemic factor influencing resilience across diverse operational environments [3] [14] [20]. It also recognizes that while workforce-related challenges may exhibit common patterns across sectors, their manifestation is mediated by sector-specific conditions, such as regulatory frameworks, technological architectures, and operational priorities [4] [16].

To address this question, the study adopts a comparative multi-sector design. Cases from transportation, finance, and telecommunications are used to identify cross-sector patterns of workforce-related constraints, including hybrid skill shortages, communication breakdowns, and delays in incident detection and response [5] [6] [18]. These patterns serve as a comparative baseline, enabling the study to distinguish between systemic challenges and those that are uniquely intensified within the energy sector, where legacy OT systems, safety-critical operations, and risk-averse regulatory cultures shape cybersecurity practice [3] [16].

Research Objectives

- To systematically synthesize the literature on cybersecurity workforce gaps and their implications for infrastructure resilience using a PRISMA-based methodology [14] [21].
- To analyze how cybersecurity workforce shortages affect operational cybersecurity practices across multiple critical infrastructure sectors, including energy, transportation, finance, and telecommunications.

- To identify both cross-sector patterns and sector-specific dynamics - particularly in the energy sector—that shape the relationship between workforce capability and resilience.
- To develop a socio-technical conceptual framework illustrating how cybersecurity workforce capability underpins resilient critical digital infrastructure [7] [8].

Table 1 highlights that, while prior work addresses frameworks and technical tools [1]-[3] [14], it often overlooks how workforce gaps disrupt operational cybersecurity in critical sectors. This study fills this gap by offering empirical evidence of these disruptions in energy, transportation, finance, and telecommunications.

Table 1. A synopsis of contributions and gaps filled in this study.

ASPECT	DETAILS
Research Gap Filled	- Addresses the lack of empirical research on how workforce shortages disrupt cybersecurity operations in critical infrastructure [14] [22] [23]. - Fills the void in cross-sectoral analysis of hybrid skill needs and operational resilience [9] [10]. - Extends beyond existing literature that focuses on technical tools or generic workforce metrics by integrating sector-specific, operational, and human factors [1] [2]. - Responds to calls for context-aware, interdisciplinary approaches to cybersecurity capability [3] [12] [20].
Contribution	- Reframes the cybersecurity workforce gap as a socio-technical resilience issue, not just a staffing problem [3] [14]. - Develops a conceptual framework grounded in Socio-Technical Systems (STS) theory to illustrate how workforce capability underpins infrastructure resilience [8] [15] [24]. - Provides empirical evidence from five critical sectors (energy, transport, finance, telecom) showing how hybrid skill shortages disrupt incident response and operational continuity [4] [22]. - Offers policy-relevant insights through a causal impact pathway linking workforce shortages to systemic vulnerabilities [12].

It integrates technical, organizational, and human dimensions into a unified framework, addressing calls for more context-aware interdisciplinary approaches to cybersecurity [12] [22]. By reconceptualizing the cybersecurity workforce gap as an issue of resilience, this study emphasizes the need for hybrid professionals who can bridge cybersecurity expertise with sector-specific knowledge.

Consequently, this research advances the field by demonstrating that workforce capacity is not a peripheral concern, but a foundational element of cybersecurity resilience in critical infrastructure systems.

2. Theoretical Background and Literature Review

Socio-Technical Systems Theory

Sociotechnical Systems (STS) theory offers a valuable foundation for understanding how human and technical factors interact in cybersecurity. Developed by Trist and Emery and expanded through various applications [7] [19], STS emphasizes that complex systems, such as those supporting critical digital infrastructures, comprise interconnected social and technical elements functioning within broader environments.

In cybersecurity, STS frames organizations not as purely technical entities but as integrated socio-technical systems in which people, processes, tools, and environmental factors collectively influence outcomes. The joint optimization principle, a core of STS, states that neither social nor technical components alone can achieve optimal results; both must evolve together. Optimizing one dimension (e.g., technology alone) may yield local benefits, but can leave the broader system suboptimal or exposed, creating a socio-technical gap [8].

STS also explains why persistent cybersecurity skill shortages are more common than hiring or training problems. Capabilities arise from alignment across skilled personnel, technology, organizational structure, and external conditions, such as regulation, culture, and policy. Critical infrastructure-from energy to finance and transportation-depends on this alignment to confront increasingly adaptive and intelligent threats.

From an STS perspective, developing a conceptual framework to analyze organizational practices across the social, technical, and environmental domains is highly applicable [3]. Cybersecurity professionals must possess not only technical expertise but also the ability to work across functions, align with organizational objectives, and integrate controls into broader mission-critical operations [14] [25].

Relevance of Socio-Technical Theory to This Study

This study adopts the STS lens to examine how cybersecurity workforce shortages affect digital infrastructure resilience. The theory is particularly relevant to the energy sector—and, by extension, other critical sectors-where legacy systems, regulatory complexity, and emerging technologies intersect. STS provides a framework for assessing how workforce gaps disrupt not just technical tasks but also the broader socio-technical system needed for resilient cybersecurity.

Literature Review

Resilience and the Cybersecurity Skills Gap

Resilience in critical digital infrastructure, particularly energy, is increasingly threatened by a persistent shortage of cybersecurity professionals. This gap is more than a technical deficit; it is a systemic risk to cybersecurity frameworks [3] [26]. Cybersecurity is not solely a technical concern, but also a managerial and economic concern [4] [5].

NIST [27] emphasizes managerial controls and staff awareness [23], while on-

going threat evolution necessitates continuous updates to skills and policies [28]. The NIST "Information Security Handbook" supports agency managers in implementing effective security programmes [28]. Furthermore, human behavior and perception influence effectiveness [17], indicating that a sociotechnical approach is essential. Skill shortages across sectors limit efforts to operationalize frameworks, especially in highly regulated and high-risk contexts, such as energy [20].

Cybersecurity Workforce Capability

Workforce capability is central to infrastructure resilience. Malatji *et al.* [3] presented a 29-domain model based on NIST [27] [29], covering areas such as cloud, IoT, and industrial cybersecurity [24], but noted critical gaps in practical applications. Khaw *et al.* [14] identified four capability pillars—individual, organizational, technological, and governmental—that form an interacting ecosystem rather than isolated skill sets.

Otoom *et al.* [30] promoted EduCERT, a collaborative educational framework for cross-sector knowledge exchanges. Security culture is also vital, yet is often overlooked in training [31]. Haney and Lutters [13] [26] highlighted the importance of cybersecurity advocates who require soft skills, such as communication and persuasion, which are underrepresented in traditional curricula.

Due to the ever-evolving nature of cybersecurity [14] [32], adaptability and continuous learning are critical. Economic incentives should also be considered to support talent retention and development [33]. Thus, workforce capability encompasses not only technical knowledge, but also culture, attitude, and economic sustainability.

Sector-Specific Cybersecurity Needs

Cybersecurity needs differ significantly by sector owing to varying industrial, technological, and regulatory contexts. In the energy sector, convergence between Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and the IoT introduces complex vulnerabilities [3]. SCADA is a type of Industrial Control System (ICS) used to monitor and control infrastructure and facility-based processes. These systems are essential for sectors such as energy, water, transportation, and manufacturing. An ICS is a broader term that includes both SCADA and Distributed Control Systems (DCSs). While SCADA involves centralized control with remote sensors and operator terminals, DCS distributes control functions across processors located near the instruments or devices that collect the data. Both play a critical role in monitoring and managing infrastructure systems [28].

Thomas and Sule [4] argued that technical skills alone cannot address these complexities. Thus, holistic frameworks that integrate compliance, safety, and risk management are required. Yeboah-Ofori and Opoku-Boateng [34] noted that multivendor environments further complicate workforce requirements, demanding expertise in interoperability and contracts.

The other sectors face parallel challenges. Healthcare contends with electronic health record systems vulnerabilities, similar to SCADA systems or issues [35].

Thus, Electronic Health Records (EHR) are digital patient records. Finance suffers from high staff turnover, which disrupts privacy and compliance [5]. Railways depend on workforce awareness to secure transport systems [6], while in e-government, skill gaps delay secure service provision [28].

Cultural perceptions are also important. Trust and user values shape adoption [24] [36], and robust frameworks can fail without management support [23]. Thus, sector-specific needs combine the technological, human, cultural, and regulatory components.

Operationalizing Cybersecurity in High-Risk Environments

High-risk regulated sectors face difficulties in translating frameworks into operational practices. Although standards exist [4], workforce shortages hamper consistent implementation. Legacy systems complicate staff efforts to apply compliance controls [3]. Orji and U-Dominic [24] underscored the need for cyber risk management in 3PLs to support social sustainability in supply chains. However, persistent challenges continue to impede cyber-security. These barriers are worth exploring further.

Friday *et al.* [18] emphasize that resilience depends on inter-firm coordination, especially as infrastructure supply chains become more integrated. Bechara and Schuch [15] show that international frameworks work only if the staff can adapt them locally. Managerial practices are essential [23], and ongoing reassessment is required to address shifting threats [32]. Behavioral factors also matter; user perceptions directly influence success [36]. Effective cybersecurity in such settings requires technical, managerial, and cultural alignments.

Emerging Themes: AI, Industry 4.0, and Cyber-Physical Convergence

New technologies have increased workforce demand. Graham [9] notes that AI-driven security requires skills in machine learning, ethics, and data science. Industry 4.0 calls for professionals who combine cybersecurity and engineering expertise [16]. Lifelong learning must be embedded in order to keep pace [10] [26].

The energy sector's shift to smart grids reflects broader trends in cyber-physical convergence in smart cities [37] and medical IoT [17], where more connected systems create greater vulnerabilities. Skills must be constantly renewed [32] and policies must support long-term learning [26]. NIST frameworks [27] [29] provide guidance, but depend on an agile, well-trained workforce.

Cross-Sector Insights and Workforce Stress

Workforce stress is an underappreciated vulnerability. Singh *et al.* [22] showed that pressure-filled environments degrade performance and cause attrition, exacerbating skill shortage. Spruit [12] suggests standardized frameworks, such as European e-Competence Framework (European e-CF), to align expectations and reduce overload. The European e-Competence Framework (e-CF) is a standardized reference that defines 40 Information Communication Technology (ICT) professional competences, helping to align roles and responsibilities across organizations and countries. It supports HR processes, such as recruitment, training, and career development, while also reducing role ambiguity by clearly outlining expectations.

Kour and Karim [6] found that railway staff are overwhelmed by compliance burdens, impacting morale. Chen and Zahedi [36] stressed that perceptions and attitudes shape stress outcomes. Lawelai *et al.* [26] proposed economic support for mental health, whereas Asbaş and Tuzlukaya [32] emphasized adaptable training to reduce burnout. Managerial commitment is crucial for creating supportive environments [17]. Addressing well-being is essential to address technical proficiency.

Implications from Extant Literature for Resilience and Policy

The literature has consistently shown that cybersecurity workforce shortages erode infrastructure resilience. Insufficient staffing delays threat detection and recovery [16], undermines compliance [4], and reduces public trust [38]. Skill gaps also hinder the adoption of advanced tools such as AI [9].

Policies alone are not sufficient. Managerial practices must align with regulatory goals [33], and financial and legislative support is necessary for workforce Orji and U-Dominic [24] advocated for policies attentive to culture and user perception. Lawelai *et al.* [26] underscored the importance of dynamic and evolving policies. Ultimately, policies should prioritize skill development, mental health, and workforce resilience to ensure secure, uninterrupted critical services.

Table 2 presents a synthesized overview of the existing research, highlighting various viewpoints on the capabilities of the cybersecurity workforce and their influence on the resilience of critical infrastructure.

Table 2. Summary of key literature insights.

Extant Literature	Main Focus	Key Findings
Malatji *et al.* [3], Cybersecurity capabilities for critical infrastructure resilience	Capability frameworks for critical infrastructure	Identify 29 domains adapted from NIST but note skills shortage
Khaw *et al.* [14], Systematic review of cybersecurity frameworks	Cybersecurity capability pillars	Highlight individual, organizational, technological, and governmental capability
Haney & Lutters [13], Cybersecurity advocates in practice	Human factors in cybersecurity	Importance of advocates with communication skills
Thomas & Sule [4], Service lens on cybersecurity continuity	Service-based approaches	Link resilience to continuity management
Graham [9], AI in cybersecurity workforce	AI skills in cybersecurity	AI integration requires new workforce competencies
Kour & Karim [6], Railway cybersecurity maturity	Cybersecurity maturity in transport	Workforce maturity is critical to protecting transport systems
Otoom *et al.* [30], EduCERT framework	Cybersecurity education ecosystems	Collaborative higher education models to build workforce skills

Continued

Bechara & Schuch [15], Global frameworks for cybersecurity resilience	Global policy frameworks	Need for local skills to implement international standards
Yeboah-Ofori & Opoku-Boateng [34], Cybercrime in evolving environments	Cybercrime frameworks	Skills needed to manage evolving energy cybercrime risk
Lawelai *et al.* [26], Smart city cybersecurity policy	Cybersecurity in smart cities	Challenge in policy and skills alignment
Mwogosi & Simba [35], Health EHR cybersecurity	Health sector cybersecurity	Electronic health records have parallel skills gaps
Singh *et al.* [22], Cybersecurity workforce stress	Workforce well-being	High stress impacts retention and resilience
Bowen *et al.* [23], NIST [27] [29]	Managerial cybersecurity controls	Management support is essential for workforce effectiveness
Anderson & Moore [39], Economics of information security	Economics of cybersecurity	Incentives and costs shape workforce development
Chen & Zahedi [36], Security perceptions and behavior	Human perceptions	Perceptions of security influence adoption of practices
Spruit [12], Competence frameworks in cybersecurity	Cybersecurity education	Proposes standardized frameworks to harmonize skills and reduce stress
Lnenicka *et al.* [37], Cybersecurity in smart cities	Smart infrastructure security	Highlights governance and cross-sector collaboration
Xenakis *et al.* [20], Addressing cybersecurity literacy	Workforce literacy programs	Recommends policy for critical infrastructure literacy skills
Stavrou & Piki [10], Lifelong learning for cybersecurity skills	Continuous learning	Emphasizes upskilling and workforce adaptability
Kandpal *et al.* [5], Cybersecurity in digital finance	Financial sector security	Underscores privacy and workforce skills gaps in fintech environments
Younies & Al-Tawil [40], Effect of cybercrime laws in UAE	Cyber legislation and operational readiness	Shows that legal frameworks require skilled enforcement personnel to be effective.
Radanliev *et al.* [41], Artificial intelligence in cybersecurity	AI-driven cybersecurity challenges	Finds emerging AI skills are essential but significantly lacking in current workforce profiles.
Rangarajan *et al.* [42], A roadmap to address burnout in cybersecurity profession	Workforce well-being	Offers multidimensional strategies to combat burnout and retain talent

Continued

Tallam [43], The Cyber Immune System	Adaptive cyber defense & resilience	Proposes adversarial testing as a mechanism to reinforce resilience—underscoring new skill paradigms
Walendy *et al.* [44], Curriculum initiative for hardware reverse engineering (HRE)	Hardware supply chain security	Advocates integrating HRE education into cybersecurity curricula to secure infrastructure
Alevizos [45], Complexity-informed cyber defenses	Organizational complexity and defense optimization	Introduces a model linking workforce planning and analytics to reduce defense complexity

Malatji *et al.* [3] and Khaw *et al.* [14] proposed comprehensive frameworks outlining the multidomain skills required to meet evolving cybersecurity challenges. Haney and Lutters [13] emphasized the importance of soft skills and human factors, while Graham [9] and Stavrou and Piki [10] highlighted competencies related to artificial intelligence and lifelong learning.

Sector-specific studies such as Kour and Karim [6] in the railway sector and Mwogosi and Simba [35] in healthcare illustrate how workforce gaps are tied to the operational context of each domain. These findings challenge generic workforce models and suggest that tailored development strategies are necessary. Similarly, Lawelai *et al.* [26] and Lnenicka *et al.* [37] explored smart cities and demonstrated how governance and policy must be aligned with evolving workforce needs.

This table also includes research on psychological well-being and stress among cybersecurity professionals. Singh *et al.* [22] and Spruit [12] showed that retention and mental health are integral to resilience, broadening the conventional focus on technical skills to encompass organizational culture and staff support.

Policies and governance are central to this process. Bowen *et al.* [23] and Bechara and Schuch [15] argue that international frameworks and managerial practices are effective only when paired with capable and well-supported personnel. Anderson and Moore [39] added an economic lens, noting how incentives and cost structures influence recruitment, training, and retention.

Collectively, **Table 2** underscores that addressing workforce gaps requires a holistic strategy that spans technical skills, sector-specific expertise, organizational well-being, and supportive policy infrastructure. A resilient cybersecurity ecosystem depends on a trained, motivated, and context-aware workforce that is supported both technically and psychologically.

Synthesis of Literature and Research Gaps

The literature review highlights a multidimensional challenge linking cybersecurity skills gaps to infrastructure resilience. Evidence from the energy, health, finance, and transportation sectors confirms that workforce capability is central to cybersecurity effectiveness. However, this capability remains inconsistently de-

veloped across sectors, weakening the overall resilience. The convergence of IT and OT, the growth of Industry 4.0, and AI adoption amplify the demand for specialized skills. However, outdated training models, fragmented educational pipelines, and weak cross-sector collaboration have hindered workforce development. Additionally, psychological strain among cybersecurity staff increases burnout and attrition risk. Policy frameworks alone cannot secure infrastructure without a skilled workforce to implement them.

Organizational and sectoral variations also prevent universal solutions. For instance, the energy sector relies on long-life cycle industrial control systems, creating mismatches with modern tools. Financial services face intense compliance and high staff turnover, and healthcare must secure systems without compromising patient care. These examples highlight the importance of sector-specific strategies.

The skills gap also interacts with supply chain risk. Many energy organizations outsource IT services but lack in-house cybersecurity expertise to assess contractor practices and compound vulnerabilities. Supplier weaknesses can become entry points for attackers, as in other sectors.

Finally, there is a lack of empirical research on how workforce shortages directly disrupt daily cybersecurity functions such as patching, scanning, detection, and response, especially in energy environments. Field studies and mixed-methods research can illuminate how technical deficits and human factors intersect in real-world settings.

In a nutshell, cybersecurity workforce capability is a crucial and under-explored component of infrastructure resilience. Future research should develop sector-specific training models, investigate educational and career pathways, and address workforce well-being and policy mechanisms to build a sustainable and adaptive cybersecurity labor force.

3. Methodology

Research Approach and Strategy

This study used a multi-method qualitative approach to examine how cybersecurity workforce shortages affect operational resilience in critical digital infrastructure sectors. The research was conducted in two phases: a Systematic Literature Review (SLR) to identify knowledge gaps, followed by empirical fieldwork, including semi-structured interviews and documentary analysis to build detailed case studies.

Adopts a structured iterative approach that enables the study to move beyond surface-level observations. This revealed deeper insights into how cybersecurity workforce shortages disrupt resilience in energy, transportation, and financial infrastructure. The integration of rigorous Systematic Literature Review (SLR) with empirical case studies allowed for the development of a context-sensitive understanding of the mechanisms through which staffing gaps, skill mismatches, and organizational structures shape cybersecurity outcomes.

Systematic Literature Review

A systematic literature review was carried out to map the current academic dis-

course on cybersecurity workforce shortages and their operational impacts. The review adhered to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to ensure transparency and replicability. PRISMA flow diagram illustrating the study selection process is shown in Figure 1.

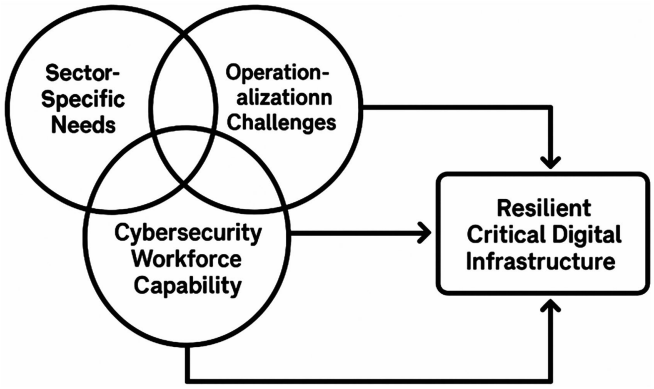

Figure 1. Conceptual framework showing how cybersecurity workforce capability interacts with sectoral demands, operational contexts, and emerging technologies to strengthen resilience in critical infrastructure.

Search Strategy and Inclusion Criteria

Databases searched included Scopus, IEEE Xplore, SpringerLink, and Emerald Insight. Articles published in English between 2015 and 2025 were eligible if they addressed the following:

- Cybersecurity workforce challenges in operational settings;
- Skill shortages or hybrid skill requirements (e.g., IT/OT convergence and AI/Machine Learning security);
- Cyber resilience or incident response in digital infrastructure.

Exclusion criteria included conceptual papers without empirical data, articles that did not focus on workforce issues, and duplicates.

Screening and Synthesis

After removing duplicates, a three-stage screening process was followed: title/abstract review, full-text assessment, and risk-of-bias appraisal using adapted CASP (Critical Appraisal Skills Programme) criteria. Articles were evaluated for methodological rigor, including research design, clarity of aims, and robustness of the findings. Studies with substantial flaws or with weak evidence were excluded.

The screening process yielded 70 articles. Three key patterns emerged:

- Workforce shortages delay incident detection and response.
- The demand for hybrid skills (e.g., cybersecurity + operational tech/data science) is increasing.
- There is limited empirical research on how shortages disrupt frontline operations.

These insights informed the second phase: fieldwork exploring real-world workforce dynamics.

PRISMA Flow Description

To ensure transparency and replicability, the study followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. The selection process is summarized below:

A total of **120 records** were initially identified across four databases (Scopus, IEEE Xplore, SpringerLink, and Emerald Insight). After removing duplicates, **95 records** remained for title and abstract screening. During this stage, **15 studies** were excluded because they were not directly related to cybersecurity workforce challenges, did not focus on critical infrastructure, or were purely conceptual without empirical evidence.

Records screened (title/abstract) (n = 95).

Records excluded (n = 15).

Reasons: Not related to workforce (n = 6); Not critical infrastructure (n = 5); Conceptual only /no empirical data (n = 4).

Full-text assessments were conducted on the remaining **80 articles**, applying inclusion criteria related to empirical relevance, methodological rigor, and focus on operational cybersecurity or resilience. At this stage, **10 studies** were excluded due to poor methodological quality, lack of relevance to resilience or operational contexts, or insufficient focus on cybersecurity workforce issues.

Full-text articles assessed (n = 80).

Full-text articles excluded (n = 10).

Reasons: Weak methodology/insufficient rigor (n = 4); Not addressing resilience or operations (n = 3); Not focused on cybersecurity workforce issues (n = 3)

The final sample consisted of **70 studies**, which formed the basis for thematic synthesis and informed the empirical phase of the research.

Qualitative Data Collection and Case Design

A multiple case study design was employed to examine socio-technical challenges in situ. Empirical material consisted of 22 semi-structured interviews and organizational documents related to cybersecurity incidents in the energy, transportation, and financial sectors.

The interviews were distributed across five cases, with each case informed by several participants according to sectoral relevance and access. Because many participants held overlapping operational responsibilities or possessed cross-sector experience, their contributions were not confined to single cases. As a result, individual interviews often provided insight that was applicable across multiple cases.

Case narratives were therefore constructed through an integration of case-specific interview data, cross-case insights, and documentary evidence. This strategy enabled analytical depth while preserving coherence with the overall sample size (n = 22).

Case Selection and Construction

The five cases were purposively selected to capture variation across critical infrastructure sectors while maintaining analytical comparability with the study's

primary focus on energy. Two cases represent the energy sector, while three cases were drawn from transportation, finance, and telecommunications to enable cross-sector comparison. Data was collected through 22 semi-structured interviews with participants occupying roles directly involved in cybersecurity operations and decision-making, including cybersecurity analysts, Security Operations Center (SOC) personnel, engineers (IT and OT), data scientists, incident response managers, and senior operational or IT managers across the respective sectors. Table 3 shows distribution of interviews across cases.

Table 3. Distribution of interviews across cases.

Case	Sector	No of interviews	Key Roles Represented
Case 1	Energy	5	OT engineers, analysts, technicians
Case 2	Energy	4	Cloud security, dispatch managers
Case 3	Transport	4	SOC analysts, rail engineers
Case 4	Finance	4	Fraud analysts, data scientists
Case 5	Telecom	5	Network engineers, SOC analysts
Total	-	**22**	-

In addition to interviews, documentary evidence was reviewed to support triangulation, including internal incident reports, security audit summaries, vulnerability assessments, policy and compliance documents, and post-incident review materials.

Each case represents a single organizational context, with the exception that minor composite elements were introduced in limited instances to protect organizational anonymity without altering the empirical patterns to preserve confidentiality and emphasize recurring socio-technical patterns. Case narratives were constructed by integrating interview data and documentary sources into coherent incident-focused accounts, allowing the analysis to capture both frontline experiences and organizational response dynamics. This approach ensures consistency across cases while enabling comparison of sector-specific and cross-sector workforce-related challenges.

Interview Protocol

Interviews were conducted over eight weeks with cybersecurity professionals, engineers, and managers. Each session lasted approximately 60 minutes and was held virtually or in person, per participant preference (see Table 3). The semi-structured guide covered the following:

- Role and responsibilities;
- Sector-specific cybersecurity challenges;
- Perceived staffing gaps and hybrid skill needs;
- Responses to recent incidents;
- Organizational barriers to action.

Sample Questions Included:

1) Describe your role in cybersecurity.

2) What challenges do you face?

3) How do staff shortages affect your work?

4) Describe recent incidents and responses.

5) What skills are missing from your team?

Interviews were recorded with consent, transcribed verbatim, anonymized, and members checked. Field notes and documents (e.g., incident reports) support triangulation.

Ethics and Consent

Ethical clearance was granted by the authors' institution. Participants received information sheets and signed informed consent forms outlining confidentiality, voluntary participation, data use, and withdrawal rights. Ethical committee contact was provided to ensure transparency.

Data Analysis

Data were analyzed using a grounded theory-inspired inductive approach. This iterative method allowed for research on surface patterns and relationships among workforce challenges, sectoral contexts, and incident response behaviors.

Coding process

Initial open coding identified concepts from the transcripts, such as "burnout," "role confusion", or "lack of authority". These were refined into four thematic categories through axial coding.

- Workforce shortages and burnout.
- Skill gaps and hybrid capability needs.
- Organizational silos and coordination issues.
- Cultural and regulatory influences on incident response.

For instance, "unclear authority" and "siloed teams" were combined under coordination breakdowns, which emerged as a critical theme across sectors. NVivo software was used to manage coding, ensure consistency, and support synthesis across the data types.

Cross-Case and Comparison Cases

While this study maintains a primary focus on the energy sector, the inclusion of transportation, finance, and telecommunications cases serves a deliberate comparative purpose. These sectors function as analytical contrasts and parallels, enabling the study to distinguish between: 1) workforce challenges that are systemic across critical infrastructure and 2) those that are uniquely shaped by the sociotechnical characteristics of the energy domain.

Through this comparative design, the study identifies recurring patterns—such as hybrid skill shortages, coordination breakdowns, and delayed incident response—as cross-sector mechanisms of resilience degradation, while also highlighting how the energy sector's reliance on legacy operational technology, safety-critical processes, and regulatory constraints intensifies these effects.

Thus, the non-energy cases do not dilute the energy focus; rather, they strengthen

causal explanation by providing comparative evidence that clarifies what is generalizable versus sector specific.

Following within-case analysis, a cross-case synthesis identified shared patterns and sector-specific differences.

- In energy, fear of triggering service disruptions (e.g., power outages) inhibited the incident response.
- In transportation, concerns focused on passenger safety and system failure-safes.
- In finance, reputational damage and regulatory compliance were dominant concerns.

All sectors converged on the challenge of lacking cross-disciplinary talent, which limited effective and timely incident responses.

Validation Strategies

To ensure analytic trustworthiness, member checking was used after each interview, allowing participants to verify the summaries. Two independent researchers reviewed the coding framework and themes to ensure inter-coder reliability. Discrepancies were resolved through discussions to enhance credibility.

4. Empirical Findings Based on Multi-Sector Case Studies

This section presents five empirical case studies of the energy, transportation, financial, and telecommunications sectors. Derived from interviews and documentary sources, they examined how cybersecurity workforce shortages disrupt incident response, coordination, and systemic resilience. Each case was interpreted through socio-technical systems theory. Pseudonyms were used where necessary. A synopsis of the case studies, presented in Table 4, serves as a prelude to the detailed presentation of the five individual cases.

Table 4. Summary of case studies.

Organization/ Sector	Incident	Frontline Perspectives	Key Implications
Energy Regional energy utility (Midwest)	Vendor credentials compromised via phishing, lateral movement into AMI/SCADA systems	Staff described being "frozen" by uncertainty; only one hybrid OT/IT expert available; field technicians afraid to act without guidance	Robust architectures ineffective without skilled cross-domain staff to coordinate incident response and avoid cascading failures
Energy "EnergyCo" (anonymized)	Malware on contractor laptop through trusted VPN, threatened dispatch scheduling	Dispatch staff torn between keeping fuel flowing and following cybersecurity instructions; confusion on escalation	Technical safeguards could not be activated under stress due to lack of hybrid cybersecurity skills and coordination bottlenecks

Continued

Transportation Metropolitan transportation authority	Vulnerability in SaaS-ICS API delayed patching for 3 months	Engineering staff felt unsupported; cybersecurity staff feared breaking safety protocols; legacy/modern teams failed to collaborate	Without cybersecurity staff trained in secure software and transportation systems, even simple vulnerabilities remain unaddressed
Finance Large financial institution	Third-party API exploited to inject adversarial data, disrupting ML fraud detection	Fraud analysts powerless to override models; cybersecurity staff lacked data science skills; delays relying on consultants	Advanced ecosystems need cybersecurity staff fluent in data science; skills shortages leave critical services vulnerable
Telecommunication National telecom provider	Phishing, ransomware, and DDoS attacks disrupted services; API misconfiguration exploited via third-party billing system	Engineers overwhelmed by alert overload; analysts lacked visibility; vendor security unknown; leadership delayed escalation	Telecom resilience depends on real-time, integrated visibility and hybrid-skilled teams across IT, OT, and vendor domains

4.1. Presentation of the Five Case Studies

Case Study 1: Third-Party Vendor Compromise in a Regional Energy Utility

A regional utility in the U.S. Midwest initiated a modernization effort integrating Advanced Metering Infrastructure (AMI) with outdated Supervisory Control and Data Acquisition (SCADA) systems. This convergence was facilitated by a third-party Internet of Things (IoT) vendor whose technicians were granted persistent Virtual Private Network (VPN) access to critical infrastructure, a common but hazardous configuration in combined Information Technology/Operational Technology (IT/OT) environments.

The incident began when a technician's credentials were compromised during a phishing attack. An attacker uses the vendor's VPN to pivot laterally into the utility network. Although network segmentation flagged unusual queries to the SCADA control panels, "*it took nearly two days to isolate the threat*". During this window, multiple internal systems are probed, triggering an operational alarm.

Interview data relating to this case indicate deep dysfunctions in incident handling. Engineers feared cutting power unintentionally by acting without a full system understanding. Analysts cannot distinguish legitimate vendor traffic from malicious activities. Only one staff member had experience in both SCADA protocols and IT security tools. This personnel shortfall left the organization vulnerable during the critical breach period.

This case highlights that even sophisticated technical defenses cannot substitute for personnel capable of interpreting and managing converged systems. This event affirms Lawelai *et al.* [26], who emphasized the need for hybrid-skilled professionals in digitally modernized utilities to uphold resilience during cyber disruptions.

Case Study 2: Malware Containment Challenges at "EnergyCo"

"EnergyCo" (pseudonym), a leading independent fuel distributor, migrated its dispatch systems to a hybrid cloud to coordinate fuel logistics across regional terminals. This transformation was intended to enhance responsiveness and real-time visibility but introduced new risks from increased interconnectivity.

The incident occurred when a contractor plugged into a personal laptop infected with malware during a VPN session. Although anomaly detection tools immediately flagged the behavior, the malware had already spread to dispatch subnets. Isolating the terminals posed a dilemma: disconnection increased the risk of halting fuel deliveries during a seasonal demand spike.

Interviews with participants in this case revealed paralyzed decisions and insufficient capacity. The only cloud security expert worked over 24 h alone, with no backup. Dispatch staff hesitated, fearing systemic service outages. Analysts deferred action owing to unclear escalation paths and segmentation knowledge gaps. A contractor reported, "*I didn't know who had authority—everyone froze*".

This case underscores that even low-sophistication malware can overwhelm organizations that lack redundancy and clear roles. Technical tools provide alerts, but skilled people are not able to interpret them under operational pressure. Delays widened the threat window and disrupted fuel supply to the entire region.

These findings reinforce Thomas and Sule [4], who argued that resilience frameworks must be underpinned by a workforce with both technical expertise and domain-specific judgment. EnergyCo's challenges illuminate human bottlenecks that persist even in cloud-mature environments.

Case Study 3: Vulnerability Management in a Metropolitan Transportation Authority

A major U.S. transit authority modernized its signaling systems, transitioning from analog infrastructure to a Communication-Based Train Control (CBTC) platform. This included integration with third-party predictive maintenance tools through Application Programming Interfaces (APIs) hosted in the cloud.

During a routine audit, a critical vulnerability was found in an API bridging the Software as a Service (SaaS) platform and on-premises training systems. This flaw enabled potential command injection into a safety-critical infrastructure. Despite the urgency, patching took over three months due to a shortage of personnel skilled in both secure software development and railway operations.

Interviews with participants in this case revealed a fractured organizational response. Security Operations Center (SOC) analysts were reluctant to act, fearing that they might disable the train safety mechanisms. One participant said, "*This wasn't a standard Linux box—we didn't know what failure looked like here*". Con-

versely, rail engineers distrusted the cybersecurity team's understanding of control systems. One commented, "*They approached this like patching a website*, *not operating a transit system*". Staff burnout is also widespread. Several employees were juggled by routine incidents and this high-risk vulnerability without sufficient support. The required cross-functional collaboration never materialized because of rigid departmental boundaries and cultural mistrust.

This case demonstrates that technically solvable vulnerabilities can remain dangerous if interdisciplinary cooperation fails. As Friday *et al*. [18] argued, effective cybersecurity in critical infrastructure demands shared mental models, not just advanced tooling. In this case, the socio-technical gap, not the flaw itself, posed the greatest threat to public safety.

Case Study 4: Adversarial Machine Learning Attack in a Financial Institution

A large national bank has adopted a Machine Learning (ML) engine to detect fraud in real time across transactions processed by financial technology (fintech) partners via API integration. The system was designed to enhance precision without delaying legitimate transactions.

Attackers exploit a misconfigured API key from the partner firm by injecting adversarial data into the model. This caused a spike in false positives, freezing thousands of legitimate transactions and triggering a customer service crisis. The incident marked a textbook example of model poisoning, a novel and poorly understood threat at the time.

Interview data relating to this case revealed confusion and slow responses. Fraud analysts lack insight into ML behavior and cannot override their decisions. Cybersecurity personnel, unfamiliar with adversarial techniques, relied on external consultants who arrived 36 hours later. A data scientist reflected, "*We couldn't explain model behavior in a way they understood*. *They thought in firewalls*, *we thought in tensors*". The absence of interdisciplinary fluency delayed containment and eroded trust between departments. Moreover, customer confidence was shaken by banks' lack of transparency and control.

This case underscores the need for hybrid-skilled professionals who can bridge the cybersecurity and artificial intelligence domains. This event supports Kandpal *et al*. [5], who call for a new skills architecture to support resilience in AI-driven financial systems. Without teams able to interpret, secure, and act on ML insights, the system's sophistication becomes a liability.

Case Study 5: Multi-Vector Cyberattacks in a National Telecom Provider

A national telecommunications company embarked on a major digital transformation to accelerate its 5G rollout and consolidate billing, customer service, and Internet of Things (IoT) management through centralized cloud infrastructure. Multiple third-party vendors have managed core systems to support rapid scaling.

Over a two-week period, the provider experienced coordinated cyberattacks involving phishing, ransomware, and Distributed Denial-of-Service (DDoS) tech-

niques. A phishing email compromised the billing administrator's credentials, enabling lateral movement into customer databases. Simultaneously, ransomware is deployed through a misconfigured API linked to a third-party billing platform. The crisis peaked when a DDoS attack took down public-facing systems, disabling mobile data in several cities.

Interviews with participants in this case revealed severe breakdowns in coordination and response. The SOC teams could not correlate with different attack vectors. One network engineer said, "*Everything was on fire—email servers, routers, billing systems—and no one knew where to start*". Executive hesitation, partly due to fear of regulatory scrutiny, delayed full-scale incident response. Vendor oversight is limited. One executive admitted, "*The billing platform was a black box—we didn't know its vulnerabilities*".

Despite previous investments in Information and Communications Technology (ICT) security, siloed teams, inadequate staffing, and fragmented monitoring have left companies vulnerable to multi-vector exploitation. Analysts have been confined to outdated threat models and lack real-time threat correlation tools.

This case validates Ncube, Sishi, and Skinner [46], who argue that systemic resilience in telecoms hinges on sociotechnical integration. Complex infrastructures require not only digital sophistication but also unified governance, interoperable teams, and continuous organizational learning. A summary of these findings is presented in **Table 3**.

4.2. Addendum on the Case Studies

The following section presents practitioners' insights from the energy sector, gathered during a focus group interview.

A key informant working in the energy sector described how recent cybersecurity incidents, specifically vendor account compromises and cross-site attacks, have exposed significant vulnerabilities within existing organizational structures. "*These aren't just technical failures*", the informant explained, "*they show how disconnected our technical defenses are from the rest of the organization*".

From the practitioner's perspective, these events have clarified that a purely technical approach to cybersecurity is no longer sufficient. "*We need people who understand both the tech and the business—who can translate risks into action across departments*", another informant emphasized. This aligns with the perspective of Haney and Lutters [13], who argue that cybersecurity advocates must "*bridge cultural and operational divides across IT, security, and business functions*".

A third participant in the focused group interview stressed that the complexity of the energy sector requires a holistic, cross-functional skill set: "*You can have the best tools in place, but if your teams don't know how to align them with real-world operations, you're still vulnerable.*" Technical controls, no matter how advanced, must be coupled with strategic human expertise and embedded within organizational policies and workflows. As the informant concluded, "*Cybersecurity resilience isn't just about firewalls and patches—it's about people, process,*

and purpose".

5. Discussion of Findings and Cross-Case Synthesis

This section interprets the empirical findings through the socio-technical systems theory, drawing from five case studies across the energy, transportation, finance, and telecommunications sectors. It explores how cybersecurity workforce challenges emerge in practice, how they differ across sectors, and what they imply for resilience in a critical digital infrastructure. In a nutshell, it is pertinent to mention that the non-energy cases function as comparative benchmarks, allowing the study to isolate which workforce-related disruptions are systemic across sectors and which are amplified by the energy sector's unique socio-technical configuration.

The discussion follows four themes based on the theoretical foundation: 1) cybersecurity workforce capability in critical infrastructure, 2) sector-specific cybersecurity needs with a focus on energy, 3) operationalization of cybersecurity protocols in high-risk environments, and 4) implications of the cybersecurity skill gap for resilience. Together, these themes were extracted from the 70 studies screened during the systematic literature review process. offers a structured analysis of systemic, cultural, and contextual barriers to effective cyber defense.

Cybersecurity Workforce Capability in Critical Infrastructure

Cybersecurity resilience is closely linked to workforce capability. All five case studies revealed that although organizations had invested in detection, segmentation, and response technologies, these tools underperformed owing to insufficient personnel to operationalize them. This supports the findings of Malatji *et al.* [3], Khaw *et al.* [14], and Otoom *et al.* [30], who argue that cybersecurity frameworks depend not on their design, but on those implementing them. They emphasized the role of higher education in the development of cybersecurity knowledge.

The need for hybrid professionals—individuals with technical cybersecurity expertise and operational familiarity—is particularly pronounced. This includes understanding Supervisory Control and Data Acquisition (SCADA) systems in energy, signaling logic in transportation, machine-learning pipelines in finance, and distributed billing systems in telecommunications. In Case 1, the staff hesitated to isolate compromised systems due to fear of triggering power outages, while in Case 4, the inability to recognize and respond to model poisoning in fraud-detection systems exposed the limits of siloed expertise. These examples support Spruit [12] and Xenakis *et al.* [20], who argued that cybersecurity is a socio-technical capacity that depends on integrated knowledge and strong cybersecurity literacy.

The hybrid capability involves more than cross-training. It requires professionals to operate confidently amid competing operational priorities, balancing technical fluency with risk communication, negotiation, and interdepartmental collaboration. As Anderson and Moore [39] and Krishna *et al.* [38] note, security failures often stem not from technical deficiencies, but from institutional distrust and communication breakdowns. Therefore, workforce development must be ap-

proached as a systems-level challenge, not just as a training issue.

Sector-Specific Cybersecurity Needs: Focus on Energy

The energy sector's unique mix of legacy Operational Technology (OT), modern Information Technology (IT), and regulatory constraints creates complex cybersecurity challenges. Both Case 1 and Case 2 revealed that key decision-makers delayed cybersecurity actions because of fear of disrupting electricity delivery or fuel logistics. In each instance, cybersecurity teams lacked sector-specific operational knowledge to assess risk tolerances, or had their warnings overridden by leaders prioritizing continuity of service.

These dynamics confirm the findings of Thomas and Sule [4], Malatji *et al.* [3], and Haleem *et al.* [16], who stressed that cybersecurity strategies in industrial sectors must account for safety-critical processes and real-time system performance. Additionally, reliance on external vendors introduces vulnerabilities, as seen in the credential compromise and malware infection initiated outside internal systems. Yeboah-Ofori and Opoku-Boateng [34] and Friday *et al.* [18] similarly highlight how third-party dependencies elevate complexity and risk, especially when trust and coordination are weak.

The regulatory culture of the energy sector further complicates incident responses. Conservative risk policies often delay action until threats reach predefined thresholds that hybrid professionals are best suited to interpret. In their absence, defaulting to caution may inadvertently prolong systemic exposure. Related findings in healthcare [35] and smart cities [26] [37] suggest that misaligned training, limited cyber literacy, and organizational silos magnify vulnerabilities in digitally dependent sectors.

Operationalizing Cybersecurity Protocols in High-Risk Environments

Applying cybersecurity protocols in high-risk settings requires more than regulatory compliance; it depends on situational awareness, institutional trust, and seamless organizational integration. Across cases, basic actions, such as patching vulnerabilities or escalating alerts, break down due to uncertainty or procedural inertia. In Case 3, a critical API vulnerability in train signaling went unpatched for months because cybersecurity and engineering teams could not agree on an acceptable risk. In Case 5, telecom staff overwhelmed by simultaneous ransomware and Distributed Denial-of-Service (DDoS) attacks failed to coordinate because of unclear escalation procedures.

These patterns echo Bechara and Schuch [15], who show that many incidents are not caused by detection failure, but by breakdowns in execution. As Friday *et al.* [18] emphasize, socio-technical misalignment—when systems outpace organizational readiness–creates implementation bottlenecks. Moreover, the literature underscores the importance of shared mental models and collaborative practices [5] [10], both of which are lacking across multiple sectors in high-stakes moments.

Effective operationalization also requires mutual trust between teams. In the absence of shared understanding, actions are delayed or avoided. These cases highlight that cybersecurity must be embedded into sector-specific workflows–developing playbooks, conducting simulations, and aligning terminology with op-

erational goals. As Khaw *et al.* [14] and Al-Hawamleh [28] argue, integration into everyday routines matters more than technical sophistication alone does.

Implications of the Cybersecurity Skills Gap on Resilience

A shortage of cybersecurity professionals undermines organizational resilience through delayed responses, underused technologies, fragmented workflows, and burnout. Each case revealed confusion and hesitation. Case 4 showed that the absence of ML-literate cybersecurity staff led to delays and reliance on consultants. Case 5 illustrates how reputational concerns discouraged action in the face of multi-vector attacks, particularly where the authority for escalation was unclear.

These symptoms reflect systemic issues beyond the staffing numbers. Singh *et al.* [22], Xenakis *et al.* [20], and Otoom *et al.* [30] highlighted how burnout, mismatches in skill deployment, and retention problems compound risk exposure. The observed hesitancy across cases often stems from ambiguity in roles and priorities, and not from a lack of will or competence. Resilience, therefore, depends not only on staffing levels, but also on the alignment of skills, authority, and situational awareness.

Resilience should be understood as the emergent quality of integrated systems-people, processes, and technologies working together under pressure. Even well-trained teams struggle when organizational culture discourages cross-functional learning or conceals risks to avoid scrutiny. The findings highlight the need for leadership models that tolerate uncertainty, empower rapid decision-making, and prioritize iterative learning. As Krishna *et al.* [38] suggested, institutional trust and shared cybersecurity ethos are foundational for translating technical capacity into resilience.

Ultimately, the cases show that resilience in critical sectors is not solely determined by technological maturity. It emerges from a sociotechnical alignment between people, tools, and contexts. Addressing the skill gap requires developing hybrid roles, building sector-specific fluency, and enhancing operational confidence. Cybersecurity must be embedded in core operations and must not be treated as an auxiliary IT function. Regulators and institutional leaders must treat workforce readiness as a measurable indicator of resilience, recognizing that the human layer is the linchpin of any cybersecurity strategy.

6. Conclusions

This study has examined how the cybersecurity workforce gap impacts the resilience and effectiveness of cybersecurity practices across critical digital infrastructures, with an emphasis on the energy sector and comparative insights from transportation, finance, and telecommunications. Drawing on a systematic literature review and five multi-sector case studies, the findings underscore a core reality: cybersecurity resilience depends not only on technological tools but also on the human capacity to deploy, interpret, and adapt them under real-world conditions.

Evidence across sectors, reinforced by existing research, reveals that the cybersecurity skills gap is not simply about insufficient headcount, but about a qualita-

tive shortfall in hybrid capacity. As Spruit [12] noted, modern cybersecurity requires professionals who can integrate technical acumen with domain-specific knowledge. This includes fluency in Supervisory Control and Data Acquisition (SCADA) systems in energy [3], safety assurance in transportation [6], financial compliance [5], and management of vendor ecosystems in telecommunications [18].

Case studies consistently show that failure to respond effectively to cyber incidents was less about technological shortcomings and more about the absence of personnel capable of coordinating, interpreting, and applying available tools in high-stakes operational environments [4] [22]. These human-centered barriers echo sociotechnical systems research, which frames resilience as the product of well-aligned technical, human, and institutional subsystems [15].

Institutional culture and sector-specific norms also shape response dynamics. In energy, risk aversion to service disruption delayed system isolation; in transportation, safety cultures prolonged vulnerability windows; in finance, siloed structures impeded rapid coordination; and in telecommunications, vendor fragmentation and reputational risk deterred timely escalation. These patterns reflect Stavrou and Piki [10], who argued that effective cybersecurity requires cohesion across cultural, operational, and technical domains.

The literature further confirms that generic training approaches fall short in critical infrastructure settings. Khaw *et al.* [14], Al-Hawamleh [28], and Xenakis *et al.* [20] have stressed the need for cross-functional, experiential, and context-specific training models that reflect operational complexity. The inclusion of telecommunications reinforces how rapid digitalization, third-party reliance, and high public exposure intensify sector-specific workforce pressure.

Thus, this study calls for systemic rethinking of cybersecurity workforce development. This is insufficient to increase the number of trained professionals. Priority must ensure the right blend of technical skills, contextual insights, and collaborative capacity. Regulatory frameworks should incorporate workforce readiness and cross-functional coordination into the resilience metrics. Academia must co-design curricula with industry, and organizations should invest in cultivating hybrid roles and interdisciplinary structures.

Ultimately, no digital infrastructure—regardless of sophistication—can achieve resilience without skilled and empowered people. Without human capacity, even the most advanced technologies remain unrealized. Bridging the cybersecurity workforce gap is not just a technical or educational goal, but also a national imperative for economic stability, public safety, and strategic security. As digital threats escalate, addressing this gap has become a defining challenge in the digital era.

6.1. Implications of This Study for Practitioners and Policymakers

This study offers important insights for practitioners and policymakers to enhance the resilience of critical digital infrastructures. The acute shortage of skilled cybersecurity professionals, especially in energy, finance, and transportation, is not merely a workforce issue but a systemic operational risk with broad conse-

quences. Addressing this risk requires moving beyond technical fixes toward greater emphasis on human capabilities, sector-specific expertise, and organizational integration.

To facilitate clear traceability: data → themes → framework; and to strengthen the theoretical contribution of this study, a mapping table (Table 5) is presented below to explicitly link each empirical theme to its corresponding component in the conceptual frameworks. This makes the theoretical development more transparent and demonstrates how the frameworks are grounded in both the empirical data and the literature.

Table 5. Mapping of empirical themes to conceptual framework components.

Empirical Theme	Description	Framework Component	Role in Framework
Workforce shortages & burnout	Insufficient staffing, overload, and delayed response	Cybersecurity Workforce Capability	Core construct (central driver of resilience)
Hybrid skill gaps	Lack of IT-OT-AI integration skills	Cybersecurity Workforce Capability	Defines quality and effectiveness of workforce
Coordination breakdowns & silos	Poor communication, unclear authority, fragmented teams	Operationalisation Challenges	Explains failure to implement security practices
Cultural & regulatory constraints	Risk aversion, compliance pressure, sector norms	Sector-Specific Needs	Shapes decision-making and response behavior
Technological complexity (AI, IoT, IT/OT convergence)	Evolving systems and threat landscape	Emerging Technologies	Creates dynamic demand for new skills

From Themes to Conceptual Framework—Linking Empirical Themes to Conceptual Framework Development

The conceptual frameworks presented in Figure 1 and Figure 2 were directly derived from the thematic analysis of the empirical data. Following axial coding, four core themes were identified: 1) workforce shortages and burnout, 2) hybrid skill gaps, 3) coordination breakdowns and organizational silos, and 4) cultural and regulatory constraints on incident response.

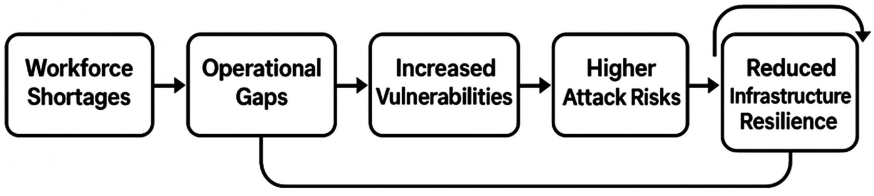

Figure 2. Conceptual framework on cybersecurity skills gap impact pathway.

These themes were systematically translated into higher-order conceptual components through an iterative abstraction process. Specifically, workforce shortages and hybrid skill gaps were integrated into the central construct of Cybersecurity Workforce Capability, representing the foundational human capacity required for resilient operations. Coordination breakdowns and organizational silos informed the component Operationalisation Challenges, capturing barriers to translating cybersecurity knowledge into effective practice. Cultural and regulatory constraints were conceptualized under Sector-Specific Needs, reflecting how institutional environments shape cybersecurity decision-making and response behavior.

In addition, insights from both the literature review and empirical cases regarding rapid technological change (e.g., AI, IoT, and IT/OT convergence) were incorporated into the component Emerging Technologies, representing evolving demands on workforce capability.

Together, these components were synthesized into an integrated socio-technical framework (**Figure 1**), illustrating how workforce capability interacts with sectoral context and operational conditions to produce resilience outcomes. The second framework (**Figure 2**) further extends this mapping by translating the same themes into a causal pathway, showing how workforce shortages lead to operational gaps, increased vulnerabilities, and ultimately reduced infrastructure resilience.

This explicit mapping (**Table 5**) ensures that the conceptual frameworks are empirically grounded and analytically traceable to the underlying data.

Unveiling a Conceptual Framework for Infrastructure Resilience

A key contribution of this study is the development of a Conceptual Framework to help practitioners and policymakers understand how cybersecurity workforce capabilities dynamically support critical infrastructure resilience. At its core, this framework positions cybersecurity workforce capability as the foundation of resilience.

The frameworks (**Figure 1** and **Figure 2**) are informed by gaps identified in the Systematic Literature Review, and challenges surfaced in five in-depth empirical case studies across the energy, transportation, financial, and telecommunications sectors. The conceptual framework in **Figure 1** offers a systems-oriented view of how cybersecurity workforce capability interacts with sectoral demands, operational contexts, and emerging technologies to reinforce resilience in a critical digital infrastructure.

At the core of the framework is Cybersecurity Workforce Capability, which represents the skills, competencies, and institutional knowledge needed to defend mission-critical systems. Based on multi-sector case studies and a Systematic Literature Review, this study shows that the workforce capability is not static. Continual development and investment are required to adapt to evolving threats, particularly in high-risk sectors such as energy, finance, and transportation.

Surrounding this central capability are three interdependent drivers:

Sector-Specific Needs

Each sector had distinct operational realities. For example, the energy sector

must secure legacy Operational Technology (OT) that converges with modern IT, while finance grapples with high-volume transactional risks and strict compliance regimes. The framework underscores that cybersecurity strategies must be tailored, and sector-specific knowledge, regulatory fluency, and mission alignment are essential.

Operationalisation Challenges

These barriers prevent cybersecurity knowledge and frameworks from being translated into sustainable practice. Legacy systems, fragmented governance, complex supply chains, and cultural divides between IT, OT, and business units hinder their execution. Cyber professionals must not only possess technical skills but also integrate security into daily operations and workflows.

Emerging Technologies

The rapid integration of artificial intelligence, blockchain, and the industrial IoT presents new opportunities and risks. As technology evolves, so do threat vectors. Without proactive upskilling, advanced tools fail to deliver resilience. The workforce must remain current, with both innovation and associated vulnerabilities.

Figure 1 visualizes these three elements as overlapping circles feeding into a Resilient Critical Digital Infrastructure, symbolizing how workforce dynamics collectively sustain resilience. This framework helps practitioners identify where targeted investments in skills, contextual knowledge, and technological readiness are urgently needed.

Importantly, feedback arrows from "Resilient Infrastructure" back to workforce capability represent an adaptive loop. A resilient environment supports continuous learning, reduces burnout, and promotes confidence, thereby allowing cybersecurity professionals to move from reactive firefighting to strategic initiatives. Strong infrastructure also reinforces the security culture and enables long-term professional development.

Thus, the framework positions the cybersecurity workforce as a linchpin connecting people, processes, and technologies. This affirms that resilience cannot be achieved through tools alone; skilled, adaptable, and sector-aware professionals are essential to designing and evolving effective cybersecurity programs for critical infrastructure.

A Conceptual Framework Mapping the Impact of Cybersecurity Skills Gaps on Infrastructure Resilience

The second framework, *the Cybersecurity Skills Gap Impact Pathway* (Figure 2), illustrates how cybersecurity workforce shortages degrade the resilience of critical digital infrastructure. Drawing from the five case studies in the energy, transport/logistics, and financial sectors, it maps a causal pathway to show how workforce gaps translate into systemic risk. The model is intended to help practitioners view workforce issues as operational and security-critical threats, rather than isolated HR challenges.

The pathway includes five sequential stages:

Workforce Shortages

All sectors examined face acute shortages of skilled cybersecurity professionals capable of managing increasingly complex cyber-physical systems. These shortcomings stem from a limited supply of qualified candidates, skill mismatches, and rapid technological changes outpacing education and training systems.

Operational Gaps

Insufficient staffing leads to delays in core functions such as patching, monitoring, incident response, and compliance. These gaps weaken cybersecurity hygiene and hinder the integration of security practices into organizational processes, particularly in sectors with converging legacy operational technology (OT) and modern Information Technology (IT).

Increased Vulnerabilities

Latent vulnerabilities persist as operational gaps persist. Systems remain unpatched, misconfigurations go unnoticed, and supply chain risks are assessed inadequately. These issues have accumulated and exposed critical systems to exploitation.

Higher Attack Risks

Unaddressed vulnerabilities increase the risk of a successful attack. Sophisticated threat actors, including ransomware groups and state-sponsored adversaries, scan for such weaknesses and target under-defended infrastructures using known tactics and procedures.

Reduced Infrastructure Resilience

Ultimately, resilience—the ability to anticipate, withstand, recover from, and adapt to cyber incidents—declines. The cumulative impact of staffing shortages and security gaps renders systems fragile and less responsive to crises.

A key feature of the framework is the feedback loop from "Reduced Infrastructure Resilience" back to "Workforce Shortages". Repeated security failures, stress, and dysfunctional response environments drive burnout, attrition, and reduced attractiveness of cybersecurity roles, compounding the skill gap. Practitioners must recognize and disrupt this cycle by prioritizing workforce well-being, training, and retention.

Figure 2 demonstrates that skill gaps are not isolated HR concerns; they propagate through operational systems, escalating into organization-wide vulnerabilities. A well-supported, cross-functionally trained cybersecurity workforce is essential for maintaining resilience in mission-critical infrastructure.

For policymakers, this framework highlights the need for sector-specific training initiatives, interdisciplinary funding strategies, and integrated workforce development programs. Resilience policies must account for not only technical standards, but also the human capacity needed to implement and adapt them.

Together, Figure 1 and Figure 2 offer a comprehensive, evidence-informed roadmap that positions cybersecurity workforce capability as the link pin of critical infrastructure resilience. Skill shortages must be treated as a foundational risk that requires coordinated strategic actions.

6.2. Theoretical Implications, Suggestions for Future Research and Limitations of This Study

Avenues for Further Research

There are several directions that merit further exploration. Thus, sector-specific workforce challenges should be examined in greater detail. While this study focused on energy, transportation, finance, and telecommunications, future research should investigate additional high-stakes domains, such as healthcare and water utilities. As Katsuya and Liu [17] and Al-Hawamleh [28] argued, each sector operates under distinct regulatory, cultural, and technical conditions that shape workforce needs.

Comparative international studies could also add value, particularly given the global disparities in cyber maturity and the workforce development infrastructure. Additionally, the role of automation and Artificial Intelligence (AI) in alleviating workforce strain deserves further study. Future research should assess how AI-based tools impact human workload, decision-making, and cognitive stress and how the governance of such tools affects training and job design.

Organizational culture and leadership practices warrant further analysis. Qualitative studies, such as ethnographies or participatory action research, could uncover how leadership attitudes toward workforce readiness influence capacity-building and response effectiveness.

Limitations of This Study

This study has several limitations. The most notable aspect is the scope of the case study sample. While diverse in sectors, the five-case dataset is not intended to be statistically representative. Broader studies with larger and more varied samples would help to validate the observed patterns.

Second, the qualitative nature of the data, based on interviews and document reviews, limits the ability to establish causality or measure the impact. While rich in context, this approach does not quantify relationships, such as between staffing levels and incident frequency.

Finally, the cybersecurity landscape has rapidly evolved. New threats, technologies, and regulations have emerged faster than many organizations can adapt. The findings offer a current snapshot, but ongoing reassessment will be essential to keep workforce strategies aligned with future risks.

Role Declaration and Funding Statement

The first author (Samuel-Noah Osarenkhoe) wrote this article in its entirety as part of his critical reflection and documentation of his experiences in his role as an IT Business Analyst and through his participation in the Executive Master of Science (MSc) in IT & Cybersecurity program at New England College in Massachusetts, USA. This study was conducted parallel to his full-time employment at Global Partner PLC, based in Waltham, Massachusetts, USA. The second author (Aihie Osarenkhoe) is an academic and therefore served solely in an advisory and corresponding author capacity during the primary author's development of the article.

Conflicts of Interest

The authors declare no financial or organizational conflicts related to the content of this manuscript.

References

[1] Allen, B., Bapst, B. and Hicks, T.A. (2023) Building a Cyber Risk Management Program: Evolving Security for the Digital Age. O'Reilly Media.

[2] Duska, K. (2025) Critical Infrastructure-Enhancing Security for Critical Infrastructure 2025.

[3] Malatji, M., Marnewick, A.L. and Von Solms, S. (2022) Cybersecurity Capabilities for Critical Infrastructure Resilience. *Information & Computer Security*, **30**, 255-279. https://doi.org/10.1108/ics-06-2021-0091

[4] Thomas, G. and Sule, M. (2023) A Service Lens on Cybersecurity Continuity and Management for Organizations' Subsistence and Growth. *Organizational Cybersecurity Journal*: *Practice*, *Process and People*, **3**, 18-40. https://doi.org/10.1108/ocj-09-2021-0025

[5] Kandpal, V., Ozili, P.K., Jeyanthi, P.M., Ranjan, D. and Chandra, D. (2025) Cybersecurity and Ensuring Privacy in Digital Finance. In: Kandpal, V., Ozili, P.K., Jeyanthi, P.M., Ranjan, D. and Chandra, D., Eds., *Digital Finance and Metaverse in Banking*, Emerald Publishing Limited, 157-170. https://doi.org/10.1108/978-1-83662-088-420251007

[6] Kour, R. and Karim, R. (2021) Cybersecurity Workforce in Railway: Its Maturity and Awareness. *Journal of Quality in Maintenance Engineering*, **27**, 453-464. https://doi.org/10.1108/jqme-07-2020-0059

[7] Baxter, G. and Sommerville, I. (2011) Socio-Technical Systems: From Design Methods to Systems Engineering. *Interacting with Computers*, **23**, 4-17. https://doi.org/10.1016/j.intcom.2010.07.003

[8] Whitworth, B. (2009) A Brief Introduction to Sociotechnical Systems. In: Khosrow-Pour, M., Ed., *Encyclopedia of Information Science and Technology*, *Second Edition*, IGI Global, 394-400. https://doi.org/10.4018/978-1-60566-026-4.ch066

[9] Graham, C.M. (2025) AI Skills in Cybersecurity: Global Job Trends Analysis. *Information & Computer Security*, **33**, 673-689. https://doi.org/10.1108/ics-09-2024-0235

[10] Stavrou, E. and Piki, A. (2024) Cultivating Self-Efficacy to Empower Professionals' Re-Up Skilling in Cybersecurity. *Information & Computer Security*, **32**, 523-541. https://doi.org/10.1108/ics-02-2024-0038

[11] U.S. Bureau of Labor Statistics (2023) Information Security Analysts. Occupational Outlook Handbook. U.S. Department of Labor.

[12] Spruit, M. (2022) Information Security Education Based on Job Profiles and the E-CF. *Higher Education*, *Skills and Work-Based Learning*, **12**, 294-308. https://doi.org/10.1108/heswbl-09-2020-0208

[13] Haney, J.M. and Lutters, W.G. (2021) Cybersecurity Advocates: Discovering the Characteristics and Skills of an Emergent Role. *Information & Computer Security*, **29**, 485-499. https://doi.org/10.1108/ics-08-2020-0131

[14] Khaw, T.Y., Amran, A. and Teoh, A.P. (2024) Building a Thematic Framework of Cybersecurity: A Systematic Literature Review Approach. *Journal of Systems and Information Technology*, **26**, 234-256. https://doi.org/10.1108/jsit-07-2023-0132

[15] Bechara, F.R. and Schuch, S.B. (2021) Cybersecurity and Global Regulatory Chal-

lenges. *Journal of Financial Crime*, **28**, 359-374.
https://doi.org/10.1108/jfc-07-2020-0149

[16] Haleem, A., Javaid, M., Singh, R.P., Rab, S. and Suman, R. (2022) Perspectives of Cybersecurity for Ameliorative Industry 4.0 Era: A Review-Based Framework. *Industrial Robot: the international journal of robotics research and application*, **49**, 582-597.
https://doi.org/10.1108/ir-10-2021-0243

[17] Katsuya, R. and Liu, X. (2025) Policy and Management Implications of Firmware Vulnerabilities in Medical IoT Devices: A Multi-Case Analysis. *Journal of Science and Technology Policy Management*, Ahead-of-Print.
https://doi.org/10.1108/jstpm-09-2024-0346

[18] Friday, D., Melnyk, S.A., Altman, M., Harrison, N. and Ryan, S. (2024) An Inductive Analysis of Collaborative Cybersecurity Management Capabilities, Relational Antecedents and Supply Chain Cybersecurity Parameters. *International Journal of Physical Distribution & Logistics Management*, **54**, 476-500.
https://doi.org/10.1108/ijpdlm-01-2023-0034

[19] Mumford, E. (2006) The Story of Socio-Technical Design: Reflections on Its Successes, Failures and Potential. *Information Systems Journal*, **16**, 317-342.
https://doi.org/10.1111/j.1365-2575.2006.00221.x

[20] Xenakis, A., Vlachos, V., Roig, P.J. and Alcaraz, S. (2025) Addressing the Necessity of Cybersecurity Literacy: The Case of ETTCS Cyberteach Project. *Information & Computer Security*, **33**, 427-451. https://doi.org/10.1108/ics-04-2024-0095

[21] Moher, D., Liberati, A., Tetzlaff, J. and Altman, D.G. (2009) Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLOS Medicine*, **6**, e1000097. https://doi.org/10.1371/journal.pmed.1000097

[22] Singh, T., Johnston, A.C., D'Arcy, J. and Harms, P.D. (2023) Stress in the Cybersecurity Profession: A Systematic Review of Related Literature and Opportunities for Future Research. *Organizational Cybersecurity Journal: Practice, Process and People*, **3**, 100-126. https://doi.org/10.1108/ocj-06-2022-0012

[23] Bowen, P., Hash, J. and Wilson, M. (2006) Information Security Handbook: A Guide for Managers. National Institute of Standards and Technology (NIST Special Publication 800-100).

[24] Orji, I.J. and U-Dominic, C.M. (2024) Modelling the Conundrums to Cyber-Risks Management in Logistics Firms for Supply Chain Social Sustainability. *Journal of Enterprise Information Management*, **37**, 1885-1925.
https://doi.org/10.1108/jeim-12-2023-0635

[25] Schreiber, A. and Schreiber, I. (2024) Bridging Knowledge Gap: The Contribution of Employees' Awareness of AI Cyber Risks Comprehensive Program to Reducing Emerging AI Digital Threats. *Information & Computer Security*, **32**, 613-635.
https://doi.org/10.1108/ics-10-2023-0199

[26] Lawelai, H., Purnomo, E.P., Nurmandi, A., Jovita, H. and Baulete, E.M. (2025) Cybersecurity Policy on Smart City Infrastructure: A Mapping of New Threats and Protections. *Journal of Science and Technology Policy Management*, Ahead-of-Print.
https://doi.org/10.1108/jstpm-09-2024-0359

[27] NIST (2017) National Institute of Standards and Technology Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations, Initial Public Draft.

[28] Al-Hawamleh, A.M. (2024) Investigating the Multifaceted Dynamics of Cybersecurity Practices and Their Impact on the Quality of E-Government Services: Evidence from the KSA. *Digital Policy, Regulation and Governance*, **26**, 317-336.

https://doi.org/10.1108/dprg-11-2023-0168

[29] NIST (2017) Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1.

[30] Otoom, A.A., Atoum, I., Al-Harahsheh, H., Aljawarneh, M., Al Refai, M.N. and Baklizi, M. (2024) A Collaborative Cybersecurity Framework for Higher Education. *Information & Computer Security*, **33**, 362-389. https://doi.org/10.1108/ics-02-2024-0048

[31] Kritzinger, E. and von Solms, S.H. (2010) Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement. *Computers & Security*, **29**, 840-847. https://doi.org/10.1016/j.cose.2010.08.001

[32] Asbaş, A.T. and Tuzlukaya, Ş. (2022) Analysis of Critical Infrastructure Resilience for Cyber-Physical Systems. *Journal of Information Security and Cybercrimes Research*, **5**, 102-114.

[33] Pipyros, K. and Liasidou, S. (2025) A New Cybersecurity Risk Assessment Framework for the Hospitality Industry: Techniques and Methods for Enhanced Data Protection and Threat Mitigation. *Worldwide Hospitality and Tourism Themes*, **17**, 48-61. https://doi.org/10.1108/whatt-12-2024-0296

[34] Yeboah-Ofori, A. and Opoku-Boateng, F.A. (2023) Mitigating Cybercrimes in an Evolving Organizational Landscape. *Continuity & Resilience Review*, **5**, 53-78. https://doi.org/10.1108/crr-09-2022-0017

[35] Mwogosi, A. and Simba, R. (2025) Digital Policy and Governance Frameworks for EHR Systems in Tanzania: A Scoping Review. *Digital Policy, Regulation and Governance*, **28**, 52-74. https://doi.org/10.1108/dprg-11-2024-0289

[36] Chen, S.P. and Redar, J.M. (2014) Ageing Workforce Knowledge Management and Transactional and Transformational Leadership: A Socio-Technical Systems Framework and a Norwegian Case Study. *International Journal of Business and Social Science*, **5**, 11-21.

[37] Lnenicka, M., Kysela, T. and Horák, O. (2025) Building Security and Resilience: A Guide to Implementing Effective Cybersecurity and Data Protection Measures in Smart Cities. *Smart and Sustainable Built Environment*, **15**, 908-937. https://doi.org/10.1108/sasbe-09-2024-0363

[38] Krishna, B., Krishnan, S. and Sebastian, M.P. (2023) Understanding the Process of Building Institutional Trust among Digital Payment Users through National Cybersecurity Commitment Trustworthiness Cues: A Critical Realist Perspective. *Information Technology & People*, **38**, 714-756. https://doi.org/10.1108/itp-05-2023-0434

[39] Anderson, R. and Moore, T. (2006) The Economics of Information Security. *Science*, **314**, 610-613. https://doi.org/10.1126/science.1130992

[40] Younies, H. and Al-Tawil, T.N. (2020) Effect of Cybercrime Laws on Protecting Citizens and Businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, **27**, 1089-1105. https://doi.org/10.1108/jfc-04-2020-0055

[41] Radanliev, P., De Roure, D., Van Kleek, M., Santos, O. and Ani, U. (2020) Artificial Intelligence in Cyber Physical Systems. *AI & SOCIETY*, **36**, 783-796. https://doi.org/10.1007/s00146-020-01049-0

[42] Rangarajan, A., Nobles, C., Dykstra, J., Cunningham, M., Robinson, N., Hollis, T., et al. (2025) A Roadmap to Address Burnout in the Cybersecurity Profession: Outcomes from a Multifaceted Workshop. In: Moallem, A., Ed., *Lecture Notes in Computer Science*, Springer Nature Switzerland, 125-140. https://doi.org/10.1007/978-3-031-92833-8_8

[43] Tallam, K. (2025) The Cyber Immune System: Harnessing Adversarial Forces for Security Resilience. arXiv:2502.17698. https://arxiv.org/abs/2502.17698

[44] Walendy, P., Koch, D. and Paar, C. (2024) A Curriculum Initiative for Hardware Reverse Engineering (HRE). In: *Proceedings of the* 2024 *Workshop on Cybersecurity Education* (*CSE*'24). Association for Computing Machinery.

[45] Alevizos, L. (2025) A Complexity-Informed Approach to Optimise Cyber Defences. Volvo Group. https://arxiv.org/pdf/2501.15578

[46] Ncube, T.R., Sishi, K.K. and Skinner, J.P. (2025) The Impact of Artificial Intelligence on Human Resource Management Practices: An Investigation. *SA Journal of Human Resource Management*, **23**, a2960. https://doi.org/10.4102/sajhrm.v23i0.2960