STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework

Osama Aljumaiah[1], Weiwei Jiang[2], Santosh Reddy Addula[3], Mohammed Amin Almaiah[4]

[1] *Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia*
[2] *Beijing University of Posts and Telecommunications, Beijing, China*
[3] *Department of Information Technology, University of the Cumberlands, Williamsburg, Kentucky, USA*
[4] *King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan*

ARTICLE INFO

Article History

Received: 01-03-2025
Revised: 22-03-2025
Accepted: 01-04-2025
Published: 04-04-2025

Academic Editor:

Prof. Youakim Badr

Vol.2025, No.2

DOI:
https://doi.org/10.63180/jcsra.thestap.2025.2.2

ABSTRACT

Due to the increasing frequency and complexity of cyberattacks in recent years, cybersecurity management has received significant attention, particularly concerning the critical infrastructure of targeted countries. Such infrastructure contains several vulnerabilities that may be readily exploited if not adequately managed. National cybersecurity regulators require critical infrastructure organizations to regularly monitor and report their cybersecurity activities. This study assesses whether the NIST framework can effectively address most threats facing critical infrastructure and identifies any notable gaps within the framework. In this literature review, most threats reported in critical infrastructure will be discussed and mapped according to the NIST cybersecurity functions, concluding with a discussion of the findings. The findings indicates that human vulnerabilities with (12 instances) represent one of the leading threats to critical infrastructure, appearing prominently in reviewed sources. Human errors, negligence, lack of awareness, insufficient training, and susceptibility to social engineering significantly increase the risk of successful cyberattacks.

Keywords: Cyberattacks, NIST framework, IT Infrastructure, Risk Analysis.

How to cite the article

Aljumaiah, O., Jiang, W., Reddy Addula, S., & Amin Almaiah, M. (2025). Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework. Journal of Cyber Security and Risk Auditing, 2025(2), 12–26. https://doi.org/10.63180/jcsra.thestap.2025.2.2

1. Introduction

The global community's understanding of cybersecurity significantly changed in 2007 following a major cyberattack on Estonia that disrupted the country's entire infrastructure [1]. Telephone services and internet networks were completely down at the peak of the crisis. Furthermore, cybersecurity incidents, such as the Stuxnet virus, have increased awareness of vulnerabilities within specialized systems controlling industrial operations (e.g., SCADA systems). Consequently, national agencies and research institutions worldwide have begun to pay greater attention to cybersecurity. This attention has led to a deeper recognition of how extensively ICT (Information and Communication Technology) infrastructure and electronic communication channels are utilized. Industrial Control Systems (ICS) are specialized ICT solutions designed primarily to support critical industrial activities [2]. These systems are responsible for monitoring and controlling a wide range of critical

*Corresponding author. Email: 222401772.student@kfu.edu.sa

infrastructure (CI). Recently, ICS have evolved to become closely interconnected with business networks and the internet [3]. As a result, they have become integral components of the cyber ecosystem, creating additional risks related to cyberattacks and cybercrime.

Cyberspace has emerged as a global catalyst for economic growth and citizen well-being. On the one hand, cyberspace offers enormous potential and significant advantages; on the other hand, vulnerabilities within cyberspace can have serious negative consequences for a country's critical infrastructure [4]. Cyberattacks and cybercrimes threaten both national security and the well-being of citizens. Attacks on a nation's critical infrastructure can severely limit state resources and undermine public trust in essential institutions [5]. Malware, cyber espionage, targeted attacks, and attacks on key information infrastructure can all negatively impact vital national interests, including national security, the economy, and infrastructure [6]. In the Kingdom of Saudi Arabia, the National Cybersecurity Authority (NCA) serves as the primary regulator for cyberspace and has implemented various initiatives to enhance cybersecurity within the Kingdom. These initiatives include requiring all government and private entities to establish cybersecurity departments to proactively address threats and vulnerabilities and protect the Kingdom's cyberspace [7]. Additionally, the NCA has established guidelines known as Essential Cybersecurity Controls (ECC) and actively promotes compliance with these controls.

A security risk management report is essential for communicating to organizational board members the significance of cybersecurity and clarifying their roles and responsibilities regarding cybersecurity systems [8]. Additionally, it's important for all organizational users to be aware of cybersecurity risks associated with systems in use, as they play a critical role in preventing cyber threats and assisting the organization in minimizing potential risks [9]. This study will explore cybersecurity risks and threats related to critical infrastructure, specifically focusing on Industrial Control Systems (ICS) and Operational Technology (OT). It aims to identify key threats and vulnerabilities within ICS and OT environments, along with effective risk mitigation strategies. Additionally, the study will utilize the NIST Cybersecurity Framework to categorize these threats and evaluate corresponding mitigation measures, ensuring comprehensive coverage and clear alignment with established cybersecurity standards. Therefore, this study provides a comprehensive literature review of cybersecurity threats targeting critical infrastructure, focusing on the effectiveness of adopting the NIST Cybersecurity Framework to enhance risk mitigation strategies. It examines existing research on identified vulnerabilities and threats within critical infrastructure sectors and evaluates how the NIST Framework contributes to addressing these cybersecurity challenges. The review aims to highlight the framework's strengths, identify any gaps, and offer insights into its practical application in protecting critical infrastructure from evolving cyber threats. This study seeks to answer the following questions:

- What are the cybersecurity threats and risks facing critical infrastructure?
- What is the impact of implementing the NIST Framework on threat mitigation within critical infrastructure?

2. Related Works

The NIST Framework begins with a three-step process: determining whether an enterprise has a formal security program and assessing its defensive capabilities; evaluating what is protected and verifying whether security procedures are effectively implemented; and ensuring that these measures are flexible, repeatable, and aligned with the organization's business objectives or mission requirements [10]. Additionally, identifying deficiencies and developing improvement plans are crucial elements of this process [11].

The author in [12] emphasizes the need for a national-level cybersecurity assurance framework to provide confidence in cybersecurity measures and prioritize areas for resource allocation. According to [13], organizations experience at least one security incident annually, leading to a global rise in cybersecurity investments, which reached 96 billion USD in 2015. Despite efforts to implement controls safeguarding Cyber-Physical Systems (CPS), major organizations continue to experience significant business disruptions due to cyberattacks. Eliminating cyberattacks entirely is extremely challenging; however, organizations should proactively anticipate threats and mitigate risks through appropriate preventive measures.

The author in [14] proposes incorporating risk prediction into comprehensive risk management practices. Effective risk analysis requires understanding the nature of cyberattacks and accurately characterizing risks by defining their origins, scope, boundaries, and the types of threats that could impact organizational objectives [15]. Additionally, as noted by [16], the growing use of information technology has heightened vulnerabilities within critical infrastructure, making

cybersecurity protection a primary concern for enterprises and governments alike. The potential operational risks posed by failing to replace aging infrastructures or not complying with regulatory standards are significant and demand attention.

Currently, known vulnerabilities attract increased attention from attackers targeting industrial systems, underscoring the need for enhanced protection. Furthermore, critical national infrastructures often experience security incidents and breaches due to human error, reinforcing the perception of people as the weakest link in cybersecurity [17]. Often, ICT equipment used in critical infrastructures consists of outdated software and hardware, which, combined with human factors, creates dangerous scenarios and exposes systems to various attacks [18].

ICS cybersecurity threats remain among the most challenging issues facing organizations, their networks, and critical assets. Organizations must accurately identify and prioritize their assets based on their importance to operations, enabling the application of targeted security measures to protect these assets [19]. Ensuring the reliability and resilience of critical infrastructures is essential to maintaining societal stability. Attackers persistently attempt to disrupt critical infrastructure availability, aiming to cause confusion and systemic harm.

The author in [20] states that cyberattacks have the potential to damage or destroy infrastructure targets remotely, anonymously, and covertly. For example, many organizations in the healthcare sector are interconnected with government entities, making data breaches particularly devastating to an entire nation. Such breaches can significantly impact public trust and the economy, as many organizations providing public services often hold government contracts and connections. The decision to integrate SCADA networks with IT networks for improved communication has made securing SCADA communications more challenging, introducing increased risks and vulnerabilities. Currently, no universally convincing methods exist to guarantee SCADA communication security.

A lack of cybersecurity awareness in managing passwords poses a critical vulnerability in ICS systems, with employees frequently failing to change or maintain default passwords [21]. Human errors and poor procedural practices contribute significantly to security breaches, highlighting the necessity of addressing personnel issues when analyzing cybersecurity risks. Ensuring safety requires robust cybersecurity practices, where effective risk management plays a pivotal role [22]. To develop and implement optimized enterprise risk management, business executives encounter various challenges. According to [1], Enterprise Risk Management Optimization (ERMO) is a methodology designed for increasingly complex and interconnected environments. ERMO can be adopted by boards, senior leadership, management, and technical practitioners to break down silos and align perspectives, thereby supporting organizational missions and business objectives. However, rapid technological advancements and market pressures often reduce decision-making timelines, leading to potentially biased solutions.

The author in [1] further argues that with recent advancements in the security field, experts and managers have evolved beyond traditional enterprise risk management (ERM) and have developed a new model known as Enterprise Security Risk Management (ESRM). ESRM strategically aligns an organization's security practices with its mission and goals using globally recognized and accepted risk management principles. Within ESRM, security risk is explicitly defined as the potential for threats to exploit vulnerabilities, causing harm, loss, or damage to organizational assets. Moreover, research in [2] investigates the impact of comprehensive risk management on company performance, demonstrating a strong correlation between effective risk management practices and organizational success. Given the critical importance of accurately assessing cybersecurity risks, especially in contexts of cybersecurity talent shortages, [3] identifies notable gaps in measuring risk levels across various domains. To address these gaps, the Multifactor Quality Measurement (MQM) approach is presented as a method to assess system limitations affecting overall security quality.

Existing cybersecurity frameworks are often complex and implementation-focused. In response, [4] proposes the PRISMA framework as an alternative methodology to evaluate cybersecurity risks within organizations. The PRISMA framework enables decision-makers to identify and operationalize customized approaches to cybersecurity risk management, assisting organizations in selecting the most suitable cybersecurity strategies for their specific situations. Investors have increasingly prioritized cybersecurity and risk management as critical considerations before investing in companies, partly driven by regulations such as those established by the American Institute of Certified Public Accountants (AICPA). Recently, the AICPA introduced a cybersecurity risk management examination service designed to offer assurance regarding the effectiveness of organizations' cybersecurity controls, addressing both rising cybersecurity threats and growing investor demand for transparent cybersecurity practices [5]. Consequently, investors now regard robust cybersecurity programs as essential criteria in their investment evaluations and decision-making processes [6].

3. Methodology

We used the PRISMA methodology to analyze research papers retrieved from the Saudi Digital Library and Google Scholar databases. The search string applied was:

(Cybersecurity risk OR cybersecurity threats) AND (critical infrastructure OR ICS)

Papers that were duplicated, not written in English, or not directly related to risk management were excluded. The search targeted academic journals and conference papers published between January 2016 and December 2022. During the identification phase, 4,681 papers were initially retrieved. In the screening phase, based on reviewing titles and abstracts, 100 papers were selected. Following a thorough full-text evaluation in the eligibility phase, 34 papers were ultimately included in this research. Relevant keywords were identified throughout the search process. Figure 1 represents the steps of PRISMA methodology.

Figure 1: PRISMA search methodology

3.1 Cybersecurity Functions Based on the NIST Framework

The NIST Cybersecurity Framework provides standardized terminology enabling various stakeholders to effectively identify, define, and manage cybersecurity risks, as shown in Table 1. It serves as a tool for aligning regulatory, business, and technological strategies to address cybersecurity challenges. The Framework can be utilized across entire organizations or specifically targeted to safeguard critical services. Additionally, sector-specific coordinating bodies, industry associations, and individual organizations can apply the Framework for diverse purposes, including compiling security reports and developing typical cybersecurity profiles. The Framework is structured around five core functions:

(1) Identify:
Develop an organizational understanding to manage cybersecurity risks related to systems, people, assets, data, and operational capabilities. Actions under the Identify function are foundational to the effective application of the Framework. Understanding the business context, critical resources, and associated cybersecurity threats enables organizations to prioritize actions aligned with their risk management strategies and business objectives. Result categories within this function include Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

(2) Protect:
Develop and implement appropriate safeguards to ensure the continued delivery of critical services. The Protect function aims to limit or contain potential cybersecurity incidents. Key categories within this function include Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

(3) Detect:
Develop and implement suitable activities to quickly identify cybersecurity incidents when they occur. Rapid detection of cybersecurity events minimizes potential damage. Result categories include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

(4) Respond:

Develop and implement effective actions to address and mitigate detected cybersecurity incidents. The Respond function supports the containment and reduction of potential damage caused by cybersecurity breaches. Categories within this function include Response Planning, Communications, Analysis, Mitigation, and Improvements.

(5) Recover:
Develop and implement plans to maintain organizational resilience and restore capabilities or services impaired due to cybersecurity incidents. The Recover function helps organizations quickly return to normal operations, reducing the long-term impact of cyber incidents. Result categories include Recovery Planning, Improvements, and Communications.

Table 1. Cybersecurity Function based on NIST framework

Cybersecurity Functions	Cybersecurity category
Identify	• ID.AM Asset Management • ID.BE Business Environment • ID.GV Governance • ID.RA Risk Assessment • ID.RM Risk Management Strategy • ID.SC Supply Chain Risk Management
Protect	• PR.AC Identity Management and Access Control • PR.AT Awareness and Training • PR.DS Data Security • PR.IP Information Protection Processes and Procedures • PR.MA Maintenance • PR.PT Protective Technology
Detect	• DE.AE Anomalies and Events • DE.CM Security Continuous Monitoring • DE.DP Detection Processes
Response	• RS.RP Response Planning • RS.CO Communications • RS.AN Analysis • RS.MI Mitigation • RS.IM Improvements
Recover	• RC.RP Recovery Planning • RC.IM Improvements • RC.CO Communications

4. Research Findings and Discussion

The findings of analysis of cybersecurity threats in critical infrastructure and Industrial Control Systems (ICS) highlights the significance of employing structured frameworks such as the NIST Cybersecurity Framework to effectively address and mitigate risks. The reviewed literature consistently identifies various cybersecurity challenges and aligns them with specific categories of the NIST framework. Table 2 represents the main findings from previous studies related to cybersecurity threats in critical infrastructure and Industrial Control Systems. Governance (ID.GV) emerges as a fundamental starting point. Shackelford et al. [21] stress the importance of having a formal security program and clearly defined defense capabilities. Similarly, Bahuguna et al. [22] emphasize that a national-level cybersecurity assurance framework provides necessary confidence and helps prioritize resources, aligning well with governance requirements outlined in the NIST framework. Miller and Grify-Brown [1] further support this, suggesting ERMO as an essential methodology to manage security risk amid complex organizational environments.

Risk Management Strategy (ID.RM) is extensively discussed, underscoring the strategic connection between cybersecurity practices and organizational goals. Marquez-Tejon et al. [2] introduce Enterprise Security Risk Management (ESRM) as a comprehensive approach that ties security efforts to business objectives. Goel et al. [5], Perols [6], and Yang et al. [7] collectively highlight the growing importance of cybersecurity risk management from an investment and regulatory perspective, demonstrating its criticality in organizational decision-making. The Business Environment (ID.BE) function draws attention to issues related to incentives and organizational performance. Casoria [23] identifies insufficient incentives as a primary cybersecurity challenge, while Mohammed and Knapkova [3] underline the correlation between effective risk management and overall company performance.

Awareness and Training (PR.AT) appears frequently in literature, reflecting the persistent human factor as a significant vulnerability. Maglaras et al. [30], Ghafir et al. [27], and Florin and Bălan [39] collectively acknowledge human errors, inadequate training, and poor cybersecurity awareness among employees as critical vulnerabilities. Murray et al. [38] and Kshetri [40] stress enhancing awareness through focused training to mitigate human-driven risks effectively. Protective Technology (PR.PT) and Security Continuous Monitoring (DE.CM) are recommended extensively by researchers like Hoffman et al. [25] and Maglaras et al. [26] as essential measures for continuously monitoring cybersecurity threats and responding proactively. Effective protection strategies and vigilant monitoring are necessary due to the increasing sophistication and frequency of cyberattacks.

Detection Processes (DE.DP) and Anomalies and Events (DE.AE) are highlighted as crucial for early identification of cybersecurity incidents. Walker-Roberts et al. [37] and Wang et al. [43] emphasize rapid detection capabilities to minimize the potential impact of breaches and malware infections, essential for preserving operational integrity and public trust. Response Planning (RS.RP), Analysis (RS.AN), and Mitigation (RS.MI) functions reflect a growing emphasis on systematic response strategies. Limba et al. [28], Lee and Shon [35], and Clark et al. [46] advocate developing comprehensive plans to swiftly contain and mitigate cyber incidents. Kumar et al. [33] and Control Engineering [45] stress analyzing and addressing vulnerabilities proactively to reduce overall exposure. Lastly, Information Protection Processes and Procedures (PR.IP) are essential for minimizing disruptions from cyberattacks, as highlighted by Shareef et al. [24], who acknowledge the difficulty of completely eliminating cyber threats but emphasize the importance of robust protective procedures In conclusion, adopting the NIST framework enables structured, strategic, and comprehensive cybersecurity risk management, providing organizations with the necessary capabilities to defend effectively against a broad spectrum of cyber threats targeting critical infrastructure.

Table 1: Finding of the mapping between cybersecurity threats with NIST cybersecurity functions

Ref	Threats Finding	Address mitigation based NIST Framework
21	The NIST Framework starts with a three-step, which is formal security program and defense capabilities." Evaluate security procedures are followed. and operational objectives and mission requirements	ID.GV Governance
22	The cybersecurity assurance framework at the country level is required to provide adequate confidence in the cybersecurity measures undertaken and to give priority areas for resource alignment.	ID.GV Governance
23	One of the major challenges of cybersecurity that arises when attempting to regulate the industry is a lack of proper incentives for users, who pay the whole expense of their security procedures.	ID.BE Business Environment
24	Organizations continue to face challenges. Cyber-attacks that might cause significant business	PR.IP Information Protection Processes and Procedures

	disruption. It is extremely difficult to remove cyber-attacks	DE.CM Security Continuous Monitoring
25	To properly deal with risk analysis, it is critical to understand the nature of cyber-attack processes and describe this risk as accurately as possible, by defining its origins, range, boundaries, and the sort of potential threats that may impact attaining the entity's goals.	PR.PT Protective Technology DE.DP Detection Processes
26	Critical National Infrastructures grow more vulnerable to cyberattacks, and protecting them becomes a critical concern for any enterprise or government.	PR.PT Protective Technology DE.CM Security Continuous Monitoring
27	Social engineering attacks have targeted organizations of various sizes and types, including those providing essential and emergency services. As more company invests in advanced IT solutions and strong encryption techniques to safeguard their data, attackers will continue to rely on old-fashioned tactics of exploiting human flaws to achieve their goals.	PR.AT Awareness and Training
1	ERMO is a methodology that considers the increasingly complex environment and interconnected.	ID.GV Governance
2	(ESRM) which can be defined as Enterprise security risk management is defined as a strategic approach to security management that ties an organization's security practices to its mission and goals using globally established and accepted risk management principles.	ID.RM Risk Management Strategy
3	Research has shown that there is a strong relationship between risk management and companies' performance.	ID.BE Business Environment
4	Notes there is so gaps in measuring the risk rating in a different area and represent The Multifactor Quality Measurement (MQM).	ID.RA Risk Assessment
5	PRISM framework that allows cyber decision-makers to identify and operationalize a personalized approach to risk management and cybersecurity issues.	ID.RM Risk Management Strategy RC.RP Recovery Planning
6	Investors on the other hand are now thinking about the cybersecurity program and risk management before the invest on that company since the government regulation.	ID.RM Risk Management Strategy
7	Investors nowadays focus on the cybersecurity program as a focal point in the investment and strength point before the decision to invest.	ID.RM Risk Management Strategy

28	Countries have not developed a strategy for responding to cyber-attacks and unanticipated events, and their vulnerabilities are underestimated. Examining cyber-security elements in the context of critical infrastructure is key to ensuring the preservation of vital national interests.	RS.RP Response Planning
29	open issues in the field of risk management Low knowledge of Risk Management operations inside public and commercial sector companies; lack of a risk management common language to improve communication across stakeholders Surveys on existing methodologies, tools, and best practices are lacking.	ID.RA Risk Assessment
30	Information security events and breaches because of human mistakes, although people are recognized as the weakest link in information security.	PR.AT Awareness and Training
31	connect SCADA networks with IT networks to provide better and quicker communication but it has consequences of cybersecurity attacks will be increased	ID.RA Risk Assessment
32	human factors and bad processes create a significant portion of security breaches	PR.AT Awareness and Training
33	The attacks are carried out by exploiting vulnerabilities in the CI's ICS systems.	RS.AN Analysis RS.MI Mitigation
34	ICS cybersecurity threat is one of the most challenging issues facing the organization, its networks, assets, and vulnerabilities. It is important to identify the assets and prioritize them	RS.MI Mitigation DE.DP Detection Processes
35	The availability of critical infrastructures should be ensured	RS.RP Response Planning RC.RP Recovery Planning
36	the (ICT) technologies equipment is often outdated software/hardware	RS.MI Mitigation
37	A data breach will have an impact on citizens' trust and the economy because many corporations that provide public services also have additional government contracts and connections.	PR.DS Data Security DE.AE Anomalies and Events
38	luck of training operational employees on cyber risk to be able to reduce behaviors, implementing cyber resilient policies, and strengthen physical security	PR.AT Awareness and Training
39	ICS Employees frequently leave default passwords on ICS systems without updating or maintaining them.	PR.AT Awareness and Training

40	lack of education about cyberattacks and awareness of their dangers among legislators and executives	PR.AT Awareness and Training DE.AE Anomalies and Events
41	The OT domain's major focus depends on the availability and integrity of ICS	RS.RP Response Planning
42	ICS systems vulnerabilities can seriously affect industrial production, life, and property safety in our daily lives.	RS.RP Response Planning
43	Attacked by highly destructive malware. This could lead to a series of consequences.	PR.DS Data Security DE.AE Anomalies and Events
44	Before implementing a gadget, evaluate its security status. Preference should be given to devices with cybersecurity certifications and goods from manufacturers who prioritize information security.	RS.IM Improvements
45	Exploiting vulnerabilities in industrial protocols, networks, and equipment is now easier than ever.	RS.AN Analysis RS.MI Mitigation
46	Cyber-attacks may include denial of service, data theft, or data modification. CI has been harmed.	PR.DS Data Security DE.DP Detection Processes
47	Enhance the detection of the vulnerability and mitigate	RS.AN Analysis RS.MI Mitigation

Figure 2 illustrates the most frequently reported threats to critical infrastructure based on the comprehensive literature review conducted in this study. Each identified threat plays a critical role in affecting the resilience and security posture of critical infrastructure systems, and these findings provide significant insights for strategic cybersecurity planning and management. The findings indicates that human vulnerabilities with (12 instances) represent one of the leading threats to critical infrastructure, appearing prominently in reviewed sources. Human errors, negligence, lack of awareness, insufficient training, and susceptibility to social engineering significantly increase the risk of successful cyberattacks.

This finding emphasizes the critical need for robust training and awareness programs targeting employees and management. These programs should not only focus on technical aspects but also on cultivating an organizational cybersecurity culture. The findings shows that lack of visibility into cybersecurity threats and weaknesses in managing such threats with (12 instances). Organizations often fail to promptly detect or adequately respond to threats due to limited monitoring, insufficient security governance, or incomplete risk management strategies. This underscores the necessity of employing effective threat detection systems, proactive monitoring, comprehensive risk management frameworks, and clear governance processes, such as the structured approach provided by the NIST cybersecurity framework. System vulnerabilities, including outdated software, inadequate protective technology, and legacy hardware and software, represent another substantial area of concern with (4 instances). Such vulnerabilities can significantly compromise system integrity and security.

This finding highlights the critical need for organizations to regularly perform vulnerability assessments, implement timely updates, patches, and adopt robust protective technologies and solutions to mitigate potential exploitation effectively. Financial-related threats, while comparatively less frequent, remain critical due to the extensive damages they could cause. The findings reveal that cyber incidents affecting financial resources or funding can lead to substantial disruption, loss of public trust, and extensive recovery costs. Organizations should incorporate financial risk considerations into cybersecurity risk assessments, ensuring they allocate sufficient financial resources for preventive and responsive cybersecurity measures. The findings show data breaches with (2 instances) present significant threats to critical infrastructure, potentially impacting operational integrity, personal and sensitive data confidentiality, and public trust. While these threats are somewhat less frequently discussed explicitly, their severe impacts underline the criticality of robust data security practices.

Organizations must implement comprehensive data protection measures such as encryption, data classification, and strong access control mechanisms. Lastly, missing or incomplete operational and security work processes contribute to a minor yet notable threat category. The absence of clearly defined cybersecurity procedures can exacerbate vulnerabilities and result in ineffective responses during cyber incidents. Addressing this threat requires organizations to develop, implement, and regularly update formal cybersecurity processes, clearly articulated policies, and procedures tailored to the operational needs of the infrastructure.

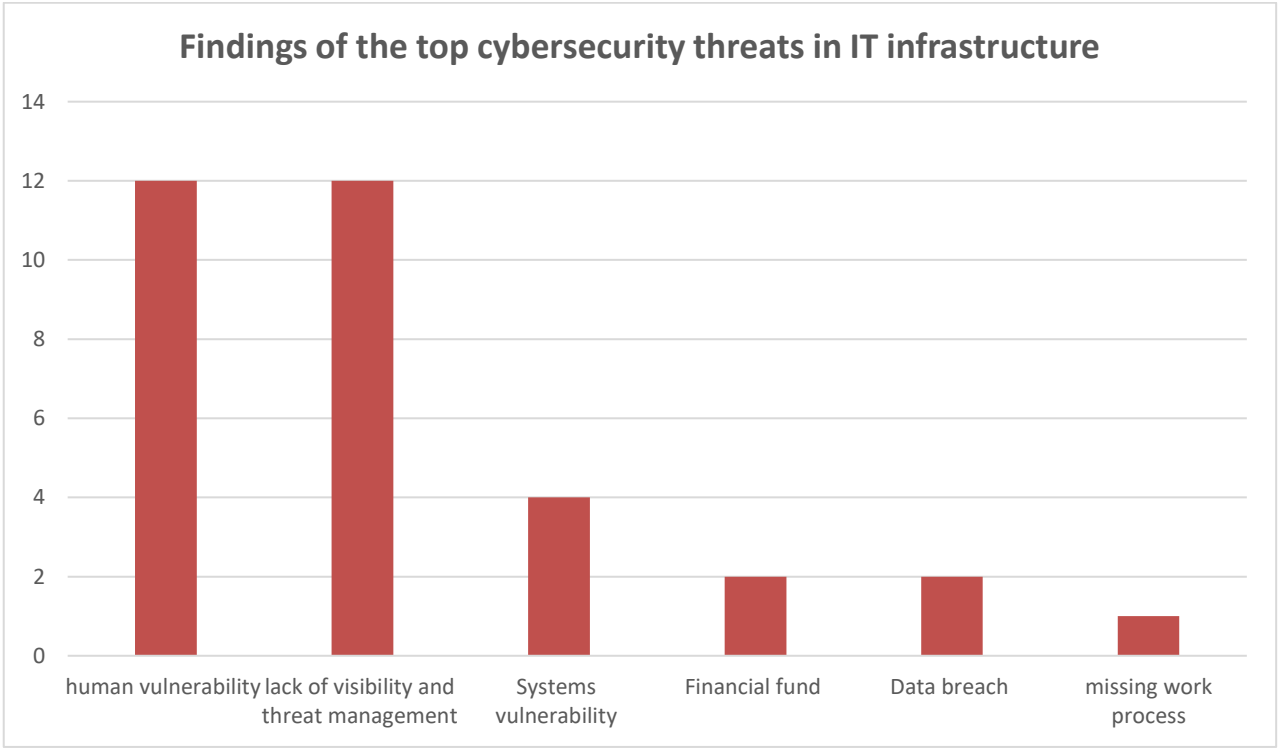


Figure 2. Findings of the top cybersecurity threats in IT infrastructure

Figure 3 represents how identified cybersecurity threats to critical infrastructure are addressed according to the five core functions of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. The distribution shown highlights where organizations and researchers currently emphasize threat mitigation efforts, based on the findings below:

Identify (28%)
The Identify function represents 28% of threat mitigation efforts, highlighting its critical role in managing cybersecurity risk. This aligns with the principle that understanding and defining cybersecurity risks—including asset management, governance, risk assessment, and strategy—is foundational to cybersecurity management. The significant emphasis on "Identify" reflects an industry consensus that proactively understanding organizational vulnerabilities and risks is essential for effective cybersecurity.

Protect (28%)
Equally, the Protect function constitutes another major portion (28%) of threat mitigation strategies. This indicates organizations heavily invest in safeguards and preventive measures, such as protective technologies, training, access control, and data protection practices. This function emphasizes that prevention remains a priority for securing critical infrastructure from various threats. Effective protection minimizes vulnerabilities and reduces the likelihood of successful cyberattacks.

Respond (23%)

The Respond function accounts for 23%, underscoring its significant role. Organizations recognize that despite robust preventive measures, incidents will still occur, making the ability to respond quickly and effectively critical. The focus on response planning, mitigation, and improvements suggests that businesses and critical infrastructure operators acknowledge the importance of preparedness and rapid action in limiting the impact of cyber incidents.

Detect (16%)
The Detect function, making up 16% of mitigation approaches, represents another vital component of a balanced cybersecurity strategy. This suggests an increasing awareness among organizations that detecting threats promptly is crucial for limiting their severity. Continuous monitoring, anomaly detection, and event identification are essential capabilities that allow organizations to proactively respond before an incident escalates.

Recover (5%)
The least represented function, Recover, comprises only 5% of the reviewed literature's mitigation strategies. While recovery planning, resilience improvements, and restoring operational capabilities are critical following cybersecurity events, the relatively lower focus might reflect a gap or oversight in many organizations' cybersecurity planning. However, considering the potentially devastating impact of successful cyberattacks, this lower emphasis could also highlight an opportunity for organizations to strengthen their recovery processes and resilience strategies.

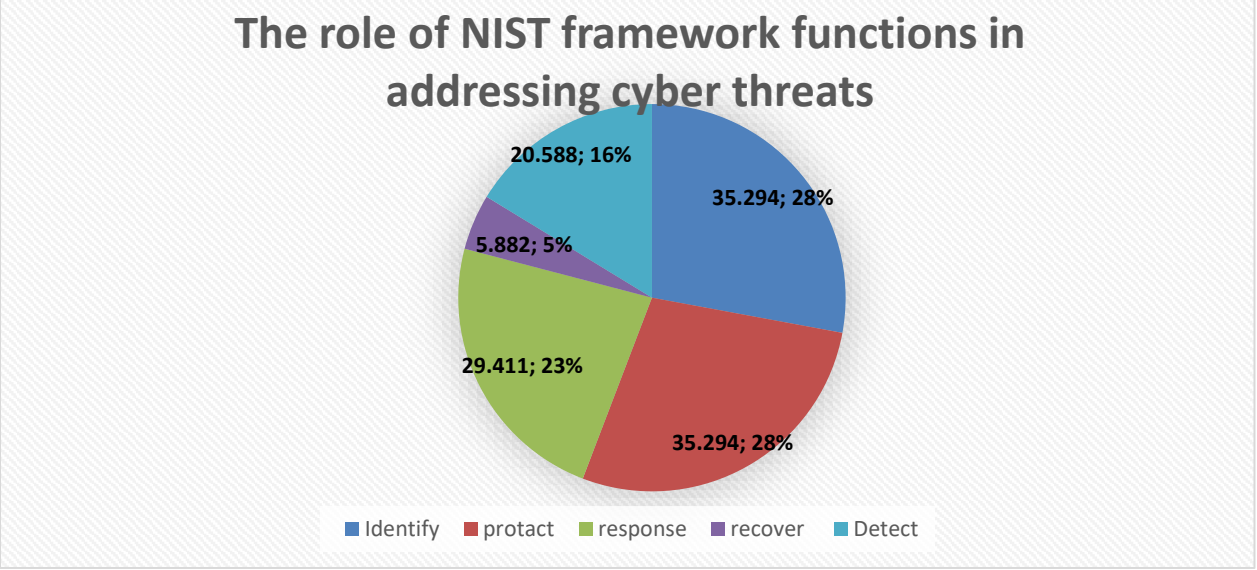


Figure 3. Findings of role of NIST framework functions in addressing cyber threats

5. Conclusion

Based on the findings of this study, critical infrastructure is vulnerable to various cybersecurity threats, which may lead to major crises affecting people and national infrastructure. This research adopted the NIST Cybersecurity Framework to address these threats. As demonstrated in Table 1, the NIST framework effectively covers all identified threats, suggesting it can resolve many cybersecurity issues. However, new and emerging threats may not yet be explicitly covered. The NIST framework is designed to be flexible and adaptable, enabling updates to address newly discovered risks.

Most threats categorized under the "Identify" function stem from deficiencies in asset management, governance, and risk management practices. Conversely, threats addressed by the "Protect" function focus primarily on safeguarding organizational assets, emphasizing human capital through training and awareness initiatives. Figure 2 highlights the most prevalent threats facing critical infrastructure systems, based on the reviewed literature. Human vulnerability emerges as the primary threat due to factors such as insufficient training, inadequate awareness, and human error, which can easily lead to severe incidents. Additionally, system vulnerabilities remain significant, mainly because critical infrastructure often

relies on outdated systems that cannot afford extensive downtime required for updates and maintenance. Furthermore, inadequate risk management practices pose substantial challenges, as cybersecurity teams must regularly conduct thorough risk assessments to identify and mitigate threats effectively.

Overall, cybersecurity is essential for mission-critical organizations. National regulations and responsible entities must take decisive actions to safeguard critical assets and protect citizens from cybersecurity threats targeting vital technologies and infrastructure.

6. Implications of the research

The research findings strongly suggest organizations managing critical infrastructure must adopt a multidimensional cybersecurity strategy. Specifically, a combined approach focusing on human factors, threat visibility, technical controls, financial resource allocation, data security, and comprehensive process management can significantly enhance an organization's resilience against cyber threats.

Integrating frameworks like the NIST Cybersecurity Framework will ensure structured, standardized, and effective management of these identified threats. Adopting such frameworks can facilitate comprehensive assessments, structured responses, and targeted improvements, ultimately strengthening the overall cybersecurity posture of critical infrastructure organizations.

On the other hand, based on the findings, the balanced distribution between the "Identify" and "Protect" functions suggests that the reviewed literature and industry practices heavily prioritize understanding and proactively safeguarding against cybersecurity threats. Nonetheless, organizations should carefully consider the lower attention given to the "Recover" function, as rapid and efficient recovery mechanisms are vital to minimizing long-term impacts of cybersecurity incidents.

Organizations should ensure comprehensive implementation of all five NIST functions, emphasizing a balanced approach that enhances organizational preparedness across the entire cybersecurity lifecycle—from identification and protection to detection, response, and recovery. This integrated strategy will effectively mitigate the cybersecurity risks that critically impact infrastructure reliability, security, and resilience.

References

[1] Herzog, S. (2017). Ten years after the Estonian cyberattacks: Defense and adaptation in the age of digital insecurity. *Geo. J. Int'l Aff.*, *18*, 67.

[2] Qin, W., Chen, S., & Peng, M. (2020). Recent advances in Industrial Internet: insights and challenges. *Digital Communications and Networks*, *6*(1), 1-13.

[3] Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D. E. A., ... & Prokop, L. (2024). Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. *Results in engineering*, 102647.

[4] Alrumaih, T. N., & Alenazi, M. J. (2025). ERINDA: A novel framework for Enhancing the Resilience of Industrial Networks against DDoS Attacks with adaptive recovery. *Alexandria Engineering Journal*, *121*, 248-262.

[5] Balta, D. D., Kaç, S. B., Balta, M., Oğur, N. B., & Eken, S. (2025). Cybersecurity-aware log management system for critical water infrastructures. *Applied Soft Computing*, *169*, 112613.

[6] Remili, K. D., Bouzourine, N., Hartani, R., & Belouchrani, A. (2025). Tech diplomacy and Critical Technologies: Case of the LEO satellite internet. *Telecommunications Policy*, 102947.

[7] Goranin, N., Čeponis, D., & Čenys, A. (2025). A Systematic Literature Review of Current Research Trends in Operational and Related Technology Threats, Threat Detection, and Security Insurance. *Applied Sciences*, *15*(5), 2316.

[8] Atıcı, S., & Tuna, G. (2025). Impact of cybersecurity attacks on electrical system operation. In *Cyber Security Solutions for Protecting and Building the Future Smart Grid* (pp. 117-160). Elsevier.

[9] Dai, J., Dai, Z., Thing, V. L., & Engineering, S. T. (2025). Cyber-Resilience Enhancement with Cross-Domain Software-Defined Network for Cyber-Physical Microgrids against Denial of Service Attacks. *IEEE Transactions on Industrial Cyber-Physical Systems*.

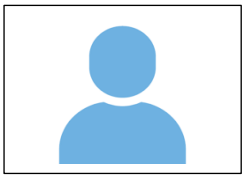
[10] Said, D. (2022). A survey on information communication technologies in modern demand-side management for smart grids: Challenges, solutions, and opportunities. *IEEE engineering management review*, *51*(1), 76-107.

[11] Möller, D. P. (2023). NIST cybersecurity framework and MITRE cybersecurity criteria. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 231-271). Cham: Springer Nature Switzerland.

[12] Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*, 100604.
[13] Gomarga, C., Winata, G. J., Thungriallu, J. E., & Wiputra, R. (2024, December). Smart Contract Security Vulnerability Through The NIST Cybersecurity Framework 2.0 Perspective. In *2024 25th International Arab Conference on Information Technology (ACIT)* (pp. 1-8). IEEE.
[14] Harish, V. S. K. V., Gupta, S., Bhatt, J. G., & Bansal, M. (2025). International standards, regulations, and best practices for cyber security of smart grid. In *Cyber Security Solutions for Protecting and Building the Future Smart Grid* (pp. 321-348). Elsevier.
[15] Gündüz, M. Z., Demirol, D., Daş, R., & Hanbay, K. (2025). Frameworks for smart grid cyber security analysis. In *Cyber Security Solutions for Protecting and Building the Future Smart Grid* (pp. 191-214). Elsevier.
[16] Busetti, S., & Scanni, F. M. (2025). Evaluating incident reporting in cybersecurity. From threat detection to policy learning. *Government Information Quarterly*, *42*(1), 102000.
[17] Ramezan, C. A. (2025). Understanding the Chief Information Security Officer: Qualifications and Responsibilities for Cybersecurity Leadership. *Computers & Security*, 104363.
[18] Padmavathi, V., & Saminathan, R. (2025). Security for the Internet of Things. In *Computer and Information Security Handbook* (pp. 353-368). Morgan Kaufmann.
[19] Latsiou, A. C., Nygård, A. R., Katsikas, S., & Lambrinoudakis, C. (2025). Never Trust-Always Verify: Assessing the cybersecurity trustworthiness of suppliers in the Digital Supply Chain. *Procedia Computer Science*, *254*, 98-107.
[20] Parmar, M., & Miles, A. (2024, May). Cyber Security Frameworks (CSFs): An Assessment Between the NIST CSF v2. 0 and EU Standards. In *2024 Security for Space Systems (3S)* (pp. 1-7). IEEE.
[21] Gomarga, C., Winata, G. J., Thungriallu, J. E., & Wiputra, R. (2024, December). Smart Contract Security Vulnerability Through The NIST Cybersecurity Framework 2.0 Perspective. In *2024 25th International Arab Conference on Information Technology (ACIT)* (pp. 1-8). IEEE.
[22] Molnar, V., & Sabodashko, D. (2024). Comparative analysis of cybersecurity in leading cloud platforms based on the NIST framework. *Social Development and Security*, *14*(6), 68-80.
[23] Lund, B. D. (2024). Blockchain Applications in Higher Education Based on the NIST Cybersecurity Framework. *Journal of Cybersecurity Education, Research and Practice*, *2024*(1).
[24] Lopes, S., Leite, P., Carvalho, S., & Teixeira, P. (2024, April). Using ITIL as part of the NIST Cybersecurity Framework. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE.
[25] Khaleefah, A. D., & Al-Mashhadi, H. M. (2024). Methodologies, requirements, and challenges of cybersecurity frameworks: A review. *Iraqi Journal of Science*, 468-486.
[27] Krumay, B., Bernroider, E. W., & Walser, R. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. In *Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23* (pp. 369-384). Springer International Publishing.
[28] Möller, D. P. (2023). NIST cybersecurity framework and MITRE cybersecurity criteria. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 231-271). Cham: Springer Nature Switzerland.
[29] White, G. B., & Sjelin, N. (2022). The NIST cybersecurity framework. In *Research anthology on business aspects of cybersecurity* (pp. 39-55). IGI Global.
[30] Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)*, *7*(3), 51-62.
[31] Delgado, M. F., Esenarro, D., Regalado, F. F. J., & Reátegui, M. D. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *3 c TIC: cuadernos de desarrollo aplicados a las TIC*, *10*(2), 123-141.
[32] Alshar'e, M. (2023). Cyber security framework selection: Comparision of NIST and ISO27001. *Applied computing Journal*, 245-255.
[33] Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gourisetti, S. N. G. (2020, October). Cyber threat dictionary using mitre att&ck matrix and nist cybersecurity framework mapping. In *2020 Resilience Week (RWS)* (pp. 106-112). IEEE.
[34] Rohan, R., Papasratorn, B., Chutimaskul, W., Hautamäki, J., Funilkul, S., & Pal, D. (2023, December). Enhancing cybersecurity resilience: A comprehensive analysis of human factors and security practices aligned with the NIST cybersecurity framework. In *Proceedings of the 13th International Conference on Advances in Information Technology* (pp. 1-16).
[35] Roy, P. P. (2020, February). A high-level comparison between the nist cyber security framework and the iso 27001 information security standard. In *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)* (pp. 1-3). IEEE.
[36] Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*, *11*(14), 2181.

[37] Koza, E. (2022). Semantic analysis of ISO/IEC 27000 standard series and NIST cybersecurity framework to outline differences and consistencies in the context of operational and strategic information security. *Med. Eng. Themes*, *2*, 26-39.
[38] Goodwin, S. (2022, March). The need for a financial sector legal standard to support the NIST Cybersecurity Framework. In *SoutheastCon 2022* (pp. 89-95). IEEE.
[39] Khaleefah, A. D., & Al-Mashhadi, H. M. (2024). Methodologies, requirements, and challenges of cybersecurity frameworks: A review. *Iraqi Journal of Science*, 468-486.
[40] Udroiu, A. M., Dumitrache, M., & Sandu, I. (2022, June). Improving the cybersecurity of medical systems by applying the NIST framework. In *2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. 1-7). IEEE.
[41] Alexander, R. D., & Panguluri, S. (2017). Cybersecurity terminology and frameworks. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, 19-47.
[42] Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP*, *4162018*(7).
[43] Maclean, D. (2017). The NIST risk management framework: Problems and recommendations. *Cyber Security: A Peer-Reviewed Journal*, *1*(3), 207-217.
[44] Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., de Sousa Júnior, R. T., & Nunes, R. R. (2021). Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology. *Ieee Access*, *9*, 129605-129618.
[45] Giuca, O., Popescu, T. M., Popescu, A. M., Prostean, G., & Popescu, D. E. (2021). A survey of cybersecurity risk management frameworks. In *Soft Computing Applications: Proceedings of the 8th International Workshop Soft Computing Applications (SOFA 2018), Vol. I 8* (pp. 240-272). Springer International Publishing.
[46] Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*, 100604.

Biographies



Osama Aljumaiah, received his M.Sc. degree in Cybersecurity from the King Faisal University (KFU), Saudi Arabia. She has published several papers in well reputed journals and conferences. Her research interests include cybersecurity, cybersecurity risk assessment and cryptographic.

Dr. Weiwei Jiang received the B.Sc. and Ph.D. degrees from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2013 and 2018, respectively. He is currently an assistant professor with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, and Key Laboratory of Universal Wireless Communications, Ministry of Education. His current research interests include artificial intelligence, machine learning, big data, wireless communication and edge computing. He has published more than 60 academic papers in IEEE Trans and other journals, with more than 3500 citations in Google Scholar. He is one of 2023 and 2024 Stanford's List of World's Top 2% Scientists.

Dr. Santosh Reddy Addula, SMIEEE, currently works as a researcher at the Department of Information Technology at the University of the Cumberlands. His research focuses on Artificial Intelligence, Machine Learning, IoT, Cybersecurity, Blockchain, Cloud Computing, Automation and Robotics, Finance, IT Healthcare and Supply Chain Management. Santosh is dedicated to advancing knowledge and developing innovative solutions in these fields. He has demonstrated expertise across multiple domains. Santosh is an innovator with a strong portfolio of patents and has significantly contributed to academic research through his articles as an author and co-author. Additionally, he serves as a reviewer for esteemed journals, reflecting his dedication to advancing knowledge and ensuring the quality of scholarly publications in his field.

Dr. Mohammed Amin Almaiah is an Associate Professor in the Department of Computer Science at University of Jordan. Almaiah is among the top 2% scientists in the world from 2020 up to now. He is working as Editor in Chief for the International Journal of Cybersecurity and Risk Assessment. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.