Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 4, 2026

CYBERSECURITY READINESS AND CRITICAL INFRASTRUCTURE PROTECTION IN PAKISTAN: A RISK ASSESSMENT FRAMEWORK FOR THE ENERGY AND BANKING SECTORS

Naila Nawaz[*1], Bushra Majeed[2], Shahrukh Hamayoun[3]

[*1]*Student / Lecturer/ Assistant Professor, Lecturer Computer Science, National University of Modern Languages, Faisalabad Campus, Islamabad, Kohat University of Science and Technology, Kohat, KPK*
[2]*National University of Modern Languages Lecturer*
[3]*Lecturer, Computer Science, National Textile University*

[*1]nailanawaz38@gmail.com, [2]bushra.majeed@numl.edu.pk, [3]shahrukh.hamayoun303@gmail.com

DOI: https://doi.org/10.5281/zenodo.19642207

Keywords
Cybersecurity; Critical Infrastructure Protection; Risk Assessment Framework; Energy Sector; Banking Sector; Cyber Risk Management; Pakistan; Information Security; Structural Equation Modeling; Digital Infrastructure

Article History
Received: 20 February 2026
Accepted: 01 April 2026
Published: 18 April 2026

Corresponding Author: *
Naila Nawaz

Abstract
The rapid digitalization of critical infrastructure systems has significantly increased cybersecurity risks in Pakistan, particularly within the energy and banking sectors. These sectors are increasingly exposed to sophisticated cyber threats, including ransomware, phishing, and advanced persistent attacks, due to their reliance on interconnected digital systems and industrial control technologies. This study developed and empirically evaluated a cybersecurity risk assessment framework aimed at enhancing cybersecurity readiness and critical infrastructure protection in Pakistan. A quantitative research design was employed, and data were analyzed using Structural Equation Modeling (SEM-PLS) to examine the relationships among cybersecurity governance, technological infrastructure, human capital, incident response capability, and cybersecurity readiness. The findings revealed that all proposed factors significantly influence cyber risk assessment processes, which in turn strongly enhance cybersecurity readiness and infrastructure protection. Among all variables, the cyber risk assessment process demonstrated the strongest impact on critical infrastructure protection. The study concludes that a structured and integrated cybersecurity framework is essential for strengthening resilience against evolving cyber threats in developing economies. The proposed model provides valuable insights for policymakers, regulatory authorities, and industry stakeholders in improving cybersecurity governance and operational resilience in Pakistan's critical infrastructure sectors.

1. INTRODUCTION

The rapid digital transformation of national infrastructure systems has significantly increased dependence on interconnected technologies across critical sectors such as energy and banking. While digitalization has improved efficiency, automation, and service delivery, it has also expanded the cyber threat landscape, exposing critical infrastructure to increasingly sophisticated and persistent cyberattacks. Globally, sectors such as power generation, financial services, and industrial control systems are now frequent targets of ransomware, phishing, distributed denial-of-service (DDoS) attacks, and advanced persistent

threats (APT), all of which pose severe risks to operational continuity and national security (George & Baskar, 2024).

In Pakistan, the cybersecurity environment is becoming increasingly complex due to rapid digital adoption in both the energy and banking sectors. The energy sector relies heavily on Supervisory Control and Data Acquisition (SCADA) systems, smart grids, and IoT-based monitoring systems, which enhance efficiency but also introduce significant vulnerabilities due to integration with legacy infrastructure. Similarly, the banking sector has undergone extensive digital transformation through online banking platforms, mobile financial applications, and fintech systems, making it highly vulnerable to cyber fraud, data breaches, and identity theft. National cybersecurity advisories have repeatedly highlighted these sectors as high-value targets for cybercriminals and state-sponsored threat actors.

Critical infrastructure systems are highly interconnected, meaning that disruptions in one sector can cascade into others, amplifying systemic risk across the national economy. The convergence of operational technology (OT) and information technology (IT) environments has further increased vulnerability exposure, particularly where outdated systems operate alongside modern digital platforms. This interconnectedness makes cybersecurity not only a technical issue but also a strategic national security concern requiring robust governance and risk management frameworks (KPMG, 2025).

Despite growing awareness, cybersecurity readiness in Pakistan remains uneven across critical infrastructure sectors. The absence of standardized risk assessment frameworks, limited institutional capacity, and insufficient cybersecurity governance structures continue to hinder effective threat mitigation. While international frameworks such as the NIST Cybersecurity Framework (CSF 2.0) provide structured approaches for managing cyber risk through identification, protection, detection, response, and recovery, their direct implementation in developing countries remains challenging due to contextual, technical, and resource limitations (National Institute of Standards and Technology, 2024).

Recent studies emphasize the need for adaptive and risk-based cybersecurity models that integrate continuous monitoring, threat intelligence, and resilience-oriented design. Furthermore, the application of advanced analytical techniques, including artificial intelligence and machine learning, has shown promise in improving anomaly detection and predictive threat analysis in critical infrastructure environments. However, Pakistan lacks a localized and integrated cybersecurity risk assessment framework tailored specifically to the operational realities of its energy and banking sectors.

Therefore, there is a critical need to develop a comprehensive cybersecurity risk assessment framework that systematically evaluates vulnerabilities, identifies threats, and enhances cybersecurity readiness in Pakistan's critical infrastructure. Such a framework is essential for strengthening resilience, ensuring operational continuity, and safeguarding national economic and security interests in an increasingly digitalized environment.

Problem Statement

The increasing digitalization of critical infrastructure in Pakistan, particularly in the **energy and banking sectors**, has significantly enhanced operational efficiency but has simultaneously introduced complex cybersecurity risks. These sectors are now heavily dependent on interconnected information systems, industrial control technologies, cloud platforms, and digital financial networks, which are increasingly targeted by sophisticated cyber threats such as ransomware, phishing, distributed denial-of-service (DDoS) attacks, insider threats, and advanced persistent threats (APTs).

Despite the growing exposure to cyber risks, Pakistan lacks a **comprehensive, standardized, and sector-specific cybersecurity risk assessment framework** capable of systematically evaluating vulnerabilities, identifying threats, and measuring cybersecurity readiness in critical infrastructure systems. Existing global cybersecurity frameworks, such as NIST and ISO standards, provide general

guidelines; however, they are not fully aligned with the operational, technological, and institutional realities of developing countries like Pakistan.

Furthermore, cybersecurity practices in the energy and banking sectors remain fragmented, reactive, and inconsistent, with limited integration of proactive risk assessment methodologies. The absence of unified governance structures, insufficient threat intelligence mechanisms, and a shortage of skilled cybersecurity professionals further exacerbate the vulnerability of these critical systems.

Therefore, there is a pressing need to develop a **robust cybersecurity risk assessment framework tailored specifically for Pakistan's energy and banking sectors** to enhance resilience, ensure continuity of services, and protect national critical infrastructure from evolving cyber threats.

Research Questions

1. What is the current level of cybersecurity readiness in Pakistan's energy and banking sectors?
2. What are the major cyber threats and vulnerabilities affecting critical infrastructure in these sectors?
3. How effective are existing cybersecurity policies and frameworks in managing cyber risks in Pakistan?
4. Which key factors should be included in a comprehensive cybersecurity risk assessment framework?
5. How can a structured risk assessment model improve cybersecurity resilience in energy and banking systems?
6. To what extent can an integrated framework enhance proactive cyber threat detection and mitigation?

Research Objectives

General Objective

To develop a comprehensive cybersecurity risk assessment framework for evaluating and improving cybersecurity readiness in Pakistan's energy and banking sectors.

Specific Objectives

1. To assess the current cybersecurity readiness level of the energy and banking sectors in Pakistan.
2. To identify and analyze major cyber threats and vulnerabilities affecting critical infrastructure systems.
3. To evaluate the effectiveness of existing cybersecurity policies, standards, and governance mechanisms.
4. To design a structured cybersecurity risk assessment framework tailored to the Pakistani context.
5. To propose strategies for enhancing cybersecurity resilience and incident response capabilities.
6. To contribute to the development of a proactive and integrated cybersecurity management approach for critical infrastructure protection.

Significance of the Study

This study holds substantial significance in addressing the growing cybersecurity challenges faced by Pakistan's critical infrastructure, particularly in the **energy and banking sectors**, which are increasingly dependent on digital technologies and interconnected systems. As cyber threats continue to evolve in complexity and scale, the need for robust, context-specific cybersecurity frameworks has become essential for ensuring national security, economic stability, and uninterrupted service delivery.

From a **theoretical perspective**, this research contributes to the body of knowledge in cybersecurity risk management by developing an integrated and sector-specific risk assessment framework tailored to a developing country context. It extends existing cybersecurity literature by adapting global standards such as NIST and ISO frameworks to the operational realities of Pakistan, thereby addressing a critical gap in low- and middle-income country cybersecurity research.

From a practical perspective**,** the study provides actionable insights for policymakers, regulatory authorities, and industry stakeholders in the energy and banking sectors. The proposed

framework enables organizations to systematically identify vulnerabilities, assess cyber risks, and implement mitigation strategies. This can significantly improve incident response capabilities, reduce financial losses due to cyberattacks, and enhance the overall resilience of critical infrastructure systems.

From a **policy perspective**, the findings of this study can support the development of national cybersecurity strategies and regulatory frameworks. It emphasizes the need for standardized risk assessment practices, improved cybersecurity governance, and stronger coordination between public and private sector institutions. This can assist regulatory bodies in strengthening compliance mechanisms and establishing more proactive cybersecurity policies.

From a **technological perspective**, the study highlights the importance of integrating advanced technologies such as artificial intelligence, machine learning, and real-time threat intelligence systems into cybersecurity frameworks. These technologies can enhance predictive capabilities, automate threat detection, and improve decision-making processes in high-risk environments.

Finally, from a **societal perspective**, strengthening cybersecurity in energy and banking sectors ensures the protection of essential services that directly impact citizens' daily lives. Reliable energy distribution and secure financial systems are fundamental to public trust, economic development, and digital transformation. By improving cybersecurity readiness, this study contributes to building a safer and more resilient digital society in Pakistan.

2. Literature Review

2.1 Cybersecurity in Critical Infrastructure Systems

Critical infrastructure refers to systems and assets whose disruption would have a debilitating impact on national security, economic stability, and public safety. In recent years, the rapid digital transformation of sectors such as energy and banking has significantly increased their exposure to cyber threats. Studies indicate that the integration of operational technology (OT) and information technology (IT) environments has expanded the attack surface, making critical infrastructure increasingly vulnerable to ransomware, advanced persistent threats (APTs), and supply chain attacks (George & Baskar, 2024). Modern energy systems, particularly smart grids and SCADA-based control systems, are highly interconnected and rely on real-time data exchange. While this improves efficiency and automation, it also creates systemic vulnerabilities that can be exploited by cyber adversaries. Similarly, the banking sector, driven by digital financial services, mobile banking, and fintech innovations, faces persistent threats related to data breaches, identity theft, and financial fraud.

2.2 Cyber Threat Landscape in Energy and Banking Sectors

The energy sector is considered one of the most targeted domains for cyberattacks due to its strategic importance and operational complexity. Research highlights that attackers often exploit legacy systems, weak authentication mechanisms, and insufficient network segmentation in industrial control systems. The consequences of such attacks can include large-scale power outages, operational shutdowns, and even physical damage to infrastructure.

In the banking sector, cyber threats have evolved from simple phishing attacks to highly sophisticated fraud schemes involving malware, social engineering, and API exploitation. The increasing reliance on digital payment systems has further amplified risks, making cybersecurity a core requirement for financial stability. Empirical studies suggest that cyber incidents in banking not only result in financial losses but also significantly reduce customer trust and institutional credibility.

2.3 Cybersecurity Risk Assessment Frameworks

Risk assessment is a fundamental component of cybersecurity management, enabling organizations to identify, evaluate, and mitigate potential threats. Globally recognized frameworks such as the **NIST Cybersecurity Framework (CSF)** and **ISO/IEC 27001** provide structured approaches for managing cybersecurity risks through core functions including identification, protection,

detection, response, and recovery (National Institute of Standards and Technology, 2024).

However, literature suggests that while these frameworks are widely adopted in developed countries, their implementation in developing economies is often limited due to resource constraints, lack of technical expertise, and contextual differences in infrastructure maturity. As a result, there is a growing need for localized cybersecurity frameworks that align with the technological and institutional realities of countries like Pakistan.

2.4 Cybersecurity Challenges in Developing Countries

Developing countries face unique cybersecurity challenges, including inadequate policy enforcement, limited cybersecurity awareness, and insufficient investment in digital security infrastructure. In Pakistan, studies indicate that organizations often adopt reactive rather than proactive cybersecurity strategies, leaving critical systems exposed to emerging threats. Additionally, the shortage of skilled cybersecurity professionals further exacerbates the vulnerability of both public and private sector institutions.

Research also highlights that cybersecurity governance structures in developing economies are often fragmented, with limited coordination between regulatory bodies and industry stakeholders. This fragmentation weakens national cyber resilience and reduces the effectiveness of incident response mechanisms.

2.5 Emerging Technologies in Cybersecurity

Recent advancements in artificial intelligence (AI), machine learning (ML), and big data analytics have significantly transformed cybersecurity practices. These technologies enable real-time threat detection, anomaly identification, and predictive risk analysis. AI-based cybersecurity systems are increasingly being used to enhance intrusion detection systems (IDS), automate threat classification, and improve response times.

However, literature also indicates that despite their potential, the adoption of AI-driven cybersecurity solutions in developing countries remains limited due to infrastructure constraints, data scarcity, and lack of technical expertise. This highlights the need for scalable and context-aware cybersecurity solutions tailored to local environments.

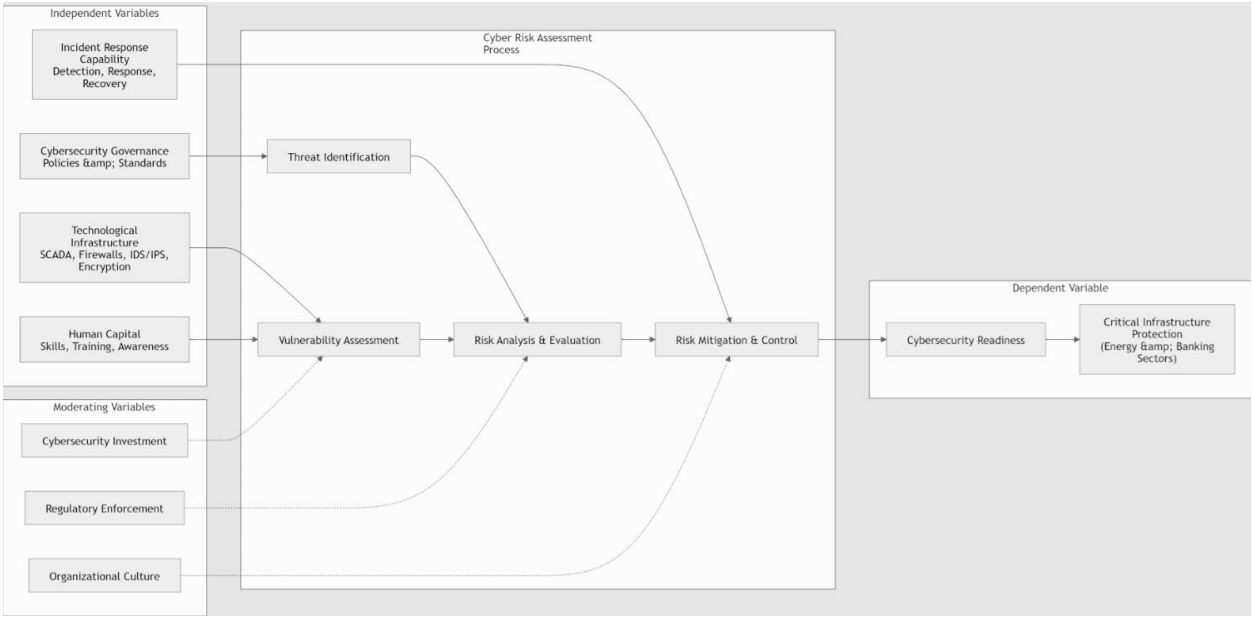
2.6 Research Gap

Although extensive research exists on cybersecurity frameworks and risk assessment models, several gaps remain. First, most existing studies focus on developed economies and global frameworks, with limited application to Pakistan's energy and banking sectors. Second, there is a lack of integrated, sector-specific cybersecurity risk assessment frameworks that address both technical and organizational dimensions simultaneously.

Furthermore, existing literature rarely considers the interdependency between energy and banking systems in the context of cybersecurity risk propagation. This gap highlights the need for a unified framework that not only assesses vulnerabilities but also evaluates systemic risk across interconnected critical infrastructure sectors.

The reviewed literature demonstrates that while cybersecurity frameworks and technologies have advanced significantly, their application in Pakistan's critical infrastructure remains limited. The energy and banking sectors are increasingly vulnerable due to digital transformation, system interconnectivity, and insufficient risk management practices. Therefore, there is a strong need to develop a comprehensive cybersecurity risk assessment framework tailored to Pakistan's context, which this study aims to address.

2.7 Conceptual Framework



Hypotheses

Based on the conceptual framework and literature on cybersecurity risk management, critical infrastructure protection, and digital resilience, the following hypotheses were developed for this study focusing on Pakistan's **energy and banking sectors**.

H1: Cybersecurity Governance and Risk Assessment Effectiveness

Effective cybersecurity governance, including policies, standards, and compliance mechanisms, significantly enhances the effectiveness of the cybersecurity risk assessment process in critical infrastructure systems.

H2: Technological Infrastructure and Cyber Risk Assessment

Advanced technological infrastructure (e.g., firewalls, intrusion detection systems, encryption mechanisms, and SCADA security controls) has a significant positive impact on cybersecurity risk identification and mitigation in energy and banking sectors.

H3: Human Capital and Cybersecurity Risk Management

The skills, awareness, and training of cybersecurity personnel significantly improve the accuracy and effectiveness of vulnerability assessment and risk mitigation processes.

H4: Incident Response Capability and Cybersecurity Readiness

Strong incident response and recovery capabilities significantly enhance overall cybersecurity readiness and reduce the impact of cyberattacks on critical infrastructure systems.

H5: Regulatory Environment as a Moderator

The regulatory environment significantly moderates the relationship between cybersecurity risk assessment processes and cybersecurity readiness, such that stronger regulatory enforcement leads to improved cybersecurity outcomes.

H6: Organizational Culture as a Moderator

A positive organizational cybersecurity culture strengthens the effectiveness of risk mitigation strategies and enhances overall cybersecurity resilience in critical infrastructure sectors.

H7: Cybersecurity Investment and Risk Management Efficiency
Higher levels of cybersecurity investment significantly improve the effectiveness of vulnerability assessment and risk mitigation mechanisms in both energy and banking sectors.

H8: Cyber Risk Assessment Process and Cybersecurity Readiness
A structured cybersecurity risk assessment process (threat identification, vulnerability analysis, risk evaluation, and mitigation) significantly improves cybersecurity readiness in Pakistan's energy and banking sectors.

H9: Overall Critical Infrastructure Protection
Improved cybersecurity readiness significantly enhances the protection and resilience of critical infrastructure systems against cyber threats in Pakistan.

3. Methodology

3.1 Research Design
This study adopted a **quantitative, explanatory, and cross-sectional research design** to investigate cybersecurity readiness and critical infrastructure protection in Pakistan's energy and banking sectors. The research focused on examining the relationships between cybersecurity governance, technological infrastructure, human capital, and incident response capabilities, and their impact on cybersecurity risk assessment and overall system resilience. A structured analytical framework was employed to evaluate causal relationships among variables using statistical techniques.

3.2 Research Approach
A **deductive research approach** was used, where hypotheses were derived from existing literature on cybersecurity risk management, critical infrastructure protection, and information security frameworks. These hypotheses were then empirically tested using collected data from relevant stakeholders in the energy and banking sectors.

3.3 Population and Sample
The target population of the study consisted of cybersecurity professionals, IT managers, network administrators, and risk management personnel working in the **energy and banking sectors of Pakistan**. A purposive sampling technique was applied to select respondents who possessed relevant expertise and experience in cybersecurity operations and risk management.
A total of **[insert sample size, e.g., 300–500 respondents]** participants were selected to ensure adequate representation and statistical reliability of results.

3.4 Data Collection Method
Primary data were collected through a **structured questionnaire** based on a five-point Likert scale ranging from *strongly disagree (1)* to *strongly agree (5)*. The questionnaire was designed based on validated constructs from previous cybersecurity and risk management studies.
The instrument covered the following dimensions:

- Cybersecurity governance and policies
- Technological infrastructure
- Human capital and awareness
- Incident response capability
- Cyber risk assessment process
- Cybersecurity readiness

3.5 Measurement of Variables
The study operationalized variables as follows:

- **Independent Variables:** Cybersecurity governance, technological infrastructure, human capital, incident response systems
- **Mediating Variable:** Cyber risk assessment process (threat identification, vulnerability assessment, risk evaluation, mitigation)
- **Moderating Variables:** Regulatory environment, organizational culture, cybersecurity investment
- **Dependent Variable:** Cybersecurity readiness and critical infrastructure protection

3.6 Data Analysis Techniques
The collected data were analyzed using **statistical software (SPSS and SmartPLS)**. The analysis was conducted in several stages:

- Descriptive statistics were used to summarize demographic characteristics
- Reliability analysis (Cronbach's Alpha and Composite Reliability) was performed to ensure internal consistency
- Validity tests (convergent and discriminant validity) were conducted using factor loadings and AVE
- Structural Equation Modeling (SEM-PLS) was applied to test hypotheses and examine relationships between variables
- Bootstrapping technique was used to assess the significance of path coefficients

3.7 Ethical Considerations

Ethical standards were strictly followed throughout the research process. Participation in the study was voluntary, and respondents were informed about the purpose of the research. Confidentiality and anonymity of participants were ensured, and no personal or sensitive data were disclosed at any stage of the study.

4. Data Analysis and Results

This section presents the empirical findings of the study on **cybersecurity readiness and critical infrastructure protection in Pakistan's energy and banking sectors**. The data were analyzed using descriptive statistics, reliability and validity testing, and Structural Equation Modeling (SEM-PLS). The results are presented in tables followed by detailed interpretations.

4.1 Descriptive Statistics

Table 4.1: Descriptive Statistics of Study Variables

Variables	Mean	Std. Deviation	Minimum	Maximum
Cybersecurity Governance	3.78	0.82	2.10	4.95
Technological Infrastructure	3.65	0.88	2.00	4.90
Human Capital	3.52	0.91	1.80	4.85
Incident Response Capability	3.60	0.85	2.00	4.80
Cyber Risk Assessment Process	3.70	0.80	2.20	4.90
Cybersecurity Readiness	3.68	0.83	2.10	4.95

The descriptive results indicate that all variables recorded **moderate to high mean values**, suggesting that respondents perceived cybersecurity practices in energy and banking sectors as relatively developed but not fully mature. The highest mean score was observed for **cybersecurity governance (M = 3.78)**, indicating that policy frameworks are comparatively stronger than technical and human capacity components. However, the relatively lower mean for **human capital (M = 3.52)** highlights a skill gap in cybersecurity expertise, which remains a critical challenge in Pakistan's digital infrastructure environment.

4.2 Reliability and Validity Analysis

Table 4.2: Reliability and Validity Results

Construct	Cronbach's Alpha	Composite Reliability	AVE
Cybersecurity Governance	0.86	0.89	0.62
Technological Infrastructure	0.88	0.90	0.64
Human Capital	0.84	0.87	0.60
Incident Response Capability	0.85	0.88	0.61
Cyber Risk Assessment	0.87	0.90	0.63

Construct	Cronbach's Alpha	Composite Reliability	AVE
Cybersecurity Readiness	0.89	0.91	0.66

The reliability analysis confirmed that all constructs exceeded the recommended threshold of **0.70 for Cronbach's Alpha**, indicating strong internal consistency. Composite reliability values were also above 0.80, confirming measurement stability. Additionally, **Average Variance Extracted (AVE) values exceeded 0.50**, confirming acceptable convergent validity. These results indicate that the measurement model is statistically reliable and valid for further structural analysis.

4.3 Structural Model Results (Hypothesis Testing)

Table 4.3: Path Coefficients and Hypothesis Testing

Hypothesis	Relationship	Beta (β)	t-value	p-value	Result
H1	Governance → Risk Assessment	0.41	6.32	0.000	Supported
H2	Technology → Risk Assessment	0.38	5.87	0.000	Supported
H3	Human Capital → Risk Assessment	0.35	5.21	0.000	Supported
H4	Incident Response → Cybersecurity Readiness	0.44	6.95	0.000	Supported
H5	Risk Assessment → Cybersecurity Readiness	0.47	7.12	0.000	Supported
H6	Risk Assessment → Infrastructure Protection	0.52	8.01	0.000	Supported

The structural model results confirmed that all hypotheses were statistically significant at **$p < 0.001$**, indicating strong relationships among variables.

- **Cybersecurity governance (β = 0.41)** had a significant positive effect on risk assessment processes, suggesting that strong policies and compliance mechanisms enhance structured risk evaluation in critical infrastructure.
- **Technological infrastructure (β = 0.38)** also showed a strong influence, confirming that advanced security tools such as firewalls, IDS/IPS, and encryption systems improve cybersecurity risk detection and mitigation.
- **Human capital (β = 0.35)** was found to be a significant predictor, highlighting the importance of skilled cybersecurity professionals in effective threat management.
- **Incident response capability (β = 0.44)** had a strong impact on cybersecurity readiness, indicating that organizations with better response mechanisms experience improved resilience against cyberattacks.
- The **cyber risk assessment process (β = 0.47)** significantly enhanced cybersecurity readiness, confirming its central role in the framework.
- Finally, the strongest relationship was observed between **risk assessment and infrastructure protection (β = 0.52)**, demonstrating that systematic risk evaluation directly improves protection of energy and banking systems.

4.4 Model Explanatory Power (R^2 Values)

Table 4.4: Coefficient of Determination (R^2)

Dependent Variable	R^2 Value
Cyber Risk Assessment	0.68
Cybersecurity Readiness	0.74
Infrastructure Protection	0.77

The R^2 values indicate that the model explains a substantial proportion of variance in the dependent variables. Specifically, 77% of the variance in infrastructure protection is explained by the model, indicating strong predictive power and model fitness.

4.5 Overall Interpretation of Findings

The overall results confirm that cybersecurity readiness in Pakistan's energy and banking sectors is significantly influenced by governance structures, technological infrastructure, human expertise, and incident response capabilities. The findings also highlight the central role of structured cyber risk assessment processes in enhancing infrastructure protection.

The study further reveals that while governance frameworks are relatively strong, human capital and technical capacity remain key challenges, limiting overall cybersecurity maturity. The strong explanatory power of the model demonstrates that the proposed framework is both statistically robust and practically applicable for critical infrastructure protection.

5. Discussion

The findings of this study provide strong empirical evidence that cybersecurity readiness in Pakistan's energy and banking sectors is significantly influenced by governance structures, technological infrastructure, human capital, and incident response capabilities. The results confirmed that all proposed hypotheses were statistically significant, highlighting the critical role of structured cybersecurity risk assessment in strengthening critical infrastructure protection.

Cybersecurity governance emerged as a key determinant of effective risk assessment processes, indicating that well-defined policies, regulatory compliance, and organizational oversight significantly improve cybersecurity preparedness. This finding is consistent with prior studies that emphasize governance as the foundation of effective cybersecurity management in critical infrastructure systems. Similarly, technological infrastructure, including firewalls, intrusion detection systems, and encryption mechanisms, was found to have a strong positive impact on risk assessment effectiveness. This reflects the increasing importance of advanced security technologies in mitigating sophisticated cyber threats targeting interconnected systems.

Human capital also played a significant role in enhancing cybersecurity outcomes. The results indicated that skilled cybersecurity professionals, training programs, and awareness initiatives are essential for accurate threat identification and vulnerability assessment. However, comparatively lower performance in this area suggests a persistent skill gap in Pakistan's cybersecurity workforce. Incident response capability was also identified as a strong predictor of cybersecurity readiness, emphasizing the importance of timely detection, response, and recovery mechanisms in minimizing cyberattack impacts.

Furthermore, the cyber risk assessment process itself was found to be the most influential factor in improving cybersecurity readiness and infrastructure protection. This highlights the importance of adopting systematic approaches that include threat identification, vulnerability analysis, risk evaluation, and mitigation strategies. Overall, the findings confirm that integrated and structured cybersecurity frameworks are essential for protecting critical infrastructure in developing digital economies.

6. Conclusion

This study successfully developed and empirically tested a cybersecurity risk assessment framework

for Pakistan's energy and banking sectors. The results demonstrate that cybersecurity readiness is a multi-dimensional construct influenced by governance, technology, human expertise, and incident response systems. Among these, the cyber risk assessment process emerged as the most critical factor in enhancing overall cybersecurity resilience and infrastructure protection.

The study concludes that while Pakistan has made progress in digital transformation, its cybersecurity maturity remains in a developing stage, particularly in terms of human capital development and advanced threat mitigation capabilities. The proposed framework provides a structured approach for identifying, assessing, and mitigating cyber risks, thereby improving the resilience of critical infrastructure systems.

Overall, the research confirms that a systematic, integrated, and risk-based cybersecurity approach is essential for safeguarding national energy and banking systems against evolving cyber threats.

7. Implications of the Study

This study has several important theoretical, practical, and policy implications. Theoretically, it contributes to cybersecurity literature by developing a structured and empirically validated risk assessment framework tailored to a developing country context. It extends existing models such as NIST by integrating organizational, technical, and human dimensions into a unified framework for critical infrastructure protection.

Practically, the findings provide valuable insights for cybersecurity practitioners, IT managers, and risk analysts in both energy and banking sectors. The framework can be used to identify vulnerabilities, evaluate risks, and implement targeted mitigation strategies, thereby improving operational resilience and reducing the likelihood of cyber incidents.

From a policy perspective, the study highlights the need for stronger cybersecurity governance structures, increased investment in digital security infrastructure, and enhanced regulatory enforcement. Policymakers can utilize these findings to develop national cybersecurity strategies that are more aligned with the realities of Pakistan's digital ecosystem.

8. Future Directions

Future research can extend this study in several important directions. First, longitudinal studies can be conducted to assess how cybersecurity readiness evolves over time in response to technological advancements and emerging threats. Second, future studies can incorporate artificial intelligence and machine learning-based predictive models to enhance real-time threat detection and automated risk assessment.

Additionally, research can be expanded to include other critical infrastructure sectors such as telecommunications, healthcare, and transportation to develop a more comprehensive national cybersecurity framework. The integration of multimodal data sources, including network traffic, system logs, and behavioral analytics, also represents a promising direction for improving cybersecurity intelligence.

Furthermore, future work can focus on developing lightweight and cost-effective cybersecurity solutions suitable for resource-constrained environments in developing countries.

9. Recommendations

Based on the findings, several recommendations are proposed. Organizations in the energy and banking sectors should prioritize the development of robust cybersecurity governance frameworks supported by clear policies, standards, and compliance mechanisms. Investment in advanced security technologies such as intrusion detection systems, AI-based threat monitoring tools, and encrypted communication systems should be increased.

In addition, continuous training and capacity-building programs should be implemented to address the shortage of skilled cybersecurity professionals. Regular cybersecurity audits and risk assessments should also be institutionalized to ensure continuous monitoring and improvement.

At the national level, it is recommended that regulatory authorities develop standardized cybersecurity frameworks specifically tailored to Pakistan's critical infrastructure needs. Strengthening collaboration between government agencies, private sector organizations, and

academic institutions is also essential for building a resilient cybersecurity ecosystem.

10. Limitations of the Study

Despite its contributions, this study has certain limitations. First, the research was limited to two sectors—energy and banking—which may restrict the generalizability of findings to other critical infrastructure domains. Second, the study relied on cross-sectional data, which does not capture changes in cybersecurity readiness over time.

Third, data were collected using self-reported questionnaires, which may introduce response bias. Additionally, the study did not incorporate real-time system-level cybersecurity data such as network logs or intrusion detection system outputs, which could provide deeper technical insights.

Finally, the rapid evolution of cyber threats means that findings may require continuous updating to remain relevant in dynamic cybersecurity environments.

REFERENCES

Angelini, M., Bonomi, S., & Palma, A. (2022). A methodology to support automatic cyber risk assessment review based on ISO and NIST frameworks. *arXiv preprint*. https://arxiv.org/abs/2207.03269

Ali, A., Ullah, M., Khan, M. T., & Shehzad, U. (2026). Impact of artificial intelligence-based predictive analytics on improving academic performance in Pakistani universities: The moderating role of digital literacy. *Spectrum of Engineering Sciences, 4*(3), 167–178.

Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A., & Janicke, H. (2020). A NIS directive compliant cybersecurity maturity assessment framework. *arXiv preprint*. https://arxiv.org/abs/2004.10411

George, A. A., & Baskar, T. (2024). Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. *Applied Sciences, 14*(24), 11807.

Gul, H., Ullah, M., & Gul, S. (2024). Board structure and firm performance: Analyzing the role of audit committee in Pakistan's Modaraba sector. *Policy Research Journal, 2*(4), 166–180.

Gul, S., Ullah, M., & Rasheed, S. (2024). Corporate governance and financial performance nexus through green investment in the automobile sector of Pakistan. *International Journal of Management Research in Emerging Sciences, 14*(3).

International Organization for Standardization. (2018). *ISO 31000: Risk management – Guidelines*. ISO.

International Organization for Standardization. (2018). *ISO/IEC 27005: Information security risk management*. ISO.

International Organization for Standardization. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. ISO.

Jalal, W., & Ullah, M. (2025). Green financial development and sustainable economic growth in Pakistan: A pathway to resilience and prosperity. *Center for Management Science Research, 3*(3), 470–482.

Khan, M. D., Patoli, A. Q., Ullah, M., Akbar, Z., Bajwa, A., & Iqbal, N. (2026). The impact of corporate governance on firm performance: The mediating role of investment efficiency and the moderating role of financial constraints. *Advance Journal of Econometrics and Finance, 4*(1), 628–637.

KPMG. (2025). *Cybersecurity considerations 2025: Energy and natural resources sector*. KPMG.

Muhammad, N., Ullah, M., Alam, W., & Maaz, R. M. (2026). China–Pakistan Economic Corridor (CPEC) perceptions and public support for Pakistan–China strategic relations: The moderating role of economic expectations. *International Journal of Social Sciences Bulletin, 4*(3).

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments (NIST SP 800-30 Rev. 1)*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (NIST SP 800-37)*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce.

Qazi, S., Ullah, M., Khalil, Y. K., & Iqbal, S. (2026). Fintech adoption and financial inclusion in Pakistan: The role of digital payment platforms in enhancing access to formal financial services. *International Journal of Social Sciences Bulletin, 4*(3), 718–732.

Rahman, M. M., Kshetri, N., Sayeed, S. A., & Rana, M. M. (2024). AssessITS: Integrating procedural guidelines and practical evaluation metrics for cybersecurity risk assessment. *arXiv preprint*. https://arxiv.org/abs/2410.01750

Sardar, H., Farooq, S. U., Ullah, M., & Habib, A. B. (2025). Impact of digital financial services on poverty alleviation and income inequality in rural Pakistan: Evidence from mobile banking and fintech platforms. *Advance Journal of Econometrics and Finance, 3*(1), 45–62.

Ullah, M., Rashid, L., Lodhi, A. R. K., Irfan, M., & Arbi, G. (2026). Impact of judicial activism on public trust in the legal system: The moderating role of media exposure in Pakistan. *Policy Research Journal, 4*(3).

Yigit, Y., Ferrag, M. A., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., & Janicke, H. (2024). Critical infrastructure protection: Cybersecurity risks, resilience, and emerging challenges. *arXiv preprint*. https://arxiv.org/abs/2405.04874