



Cybersecurity Challenges in Pakistan's Financial Sector

Mubashir Ali

ma8866178@gmail.com

Received: 12 Sep 2026; Received in revised form: 10 Oct 2026; Accepted: 16 Oct 2026; Available online: 20 Oct 2026

Abstract – The rapid digital transformation of Pakistan's financial sector has significantly improved banking efficiency, financial inclusion, and customer convenience through the adoption of internet banking, mobile banking, fintech services, and digital payment systems. However, this digital expansion has simultaneously increased exposure to cybersecurity threats, making cybersecurity a critical concern for financial institutions. This study investigates the major cybersecurity challenges affecting Pakistan's financial sector, examines their impact on financial institutions and customers, evaluates the effectiveness of existing cybersecurity frameworks and regulatory measures, and proposes strategies to strengthen cybersecurity resilience. Using a qualitative research approach based on secondary data analysis, the study reviews literature, regulatory guidelines, industry reports, and international cybersecurity frameworks, including those of the State Bank of Pakistan (SBP), ISO/IEC 27001, and the NIST Cybersecurity Framework. The findings reveal that rapid digitalization has expanded the attack surface of financial institutions, with phishing attacks emerging as the most prevalent threat. Other significant risks include ransomware, data breaches, insider threats, and third-party vulnerabilities. While regulatory initiatives and international cybersecurity standards have improved governance and risk management practices, challenges such as a shortage of cybersecurity professionals, limited awareness, and uneven cybersecurity maturity persist. The study concludes that strengthening cybersecurity governance, enhancing workforce capacity, promoting cybersecurity awareness, and investing in advanced security technologies are essential for ensuring the resilience, stability, and trustworthiness of Pakistan's evolving digital financial ecosystem.

Keywords – Cybersecurity, Financial Sector, Pakistan, Digital Banking, Phishing Attacks, Cyber Resilience, Financial Technology (FinTech), Data Breaches, Regulatory Frameworks, NIST Cybersecurity Framework, ISO/IEC 27001, Digital Transformation, Cyber Risk Management, Financial Inclusion, Information Security.

I. INTRODUCTION

Over the last decade, the financial sector in Pakistan has undergone tremendous digital transformation, which has been driven by the development of information technology, financial inclusion policies, and the growth of digital services. Internet banking, mobile banking applications, digital wallets, and branchless banking solutions are now available at commercial banks, fintech companies and payment platforms (Shrestha, 2025).

Raast instant payment system of State Bank of Pakistan has further bolstered real-time digital transactions (Bokhari, 2022). These advancements have made things more efficient, more accessible, more convenient; but they've also introduced an increased risk of cybersecurity issues. This has made cybersecurity a critical aspect of safeguarding sensitive information, bolstering financial stability, and preserving trust in the digital financial landscape.

Research Objectives

This study aims to:

1. To identify the major cybersecurity challenges affecting Pakistan's financial sector.
2. To examine the impact of cyber threats on financial institutions and customers.
3. To evaluate the effectiveness of existing cybersecurity frameworks and regulatory measures.
4. To recommend strategies for enhancing cybersecurity resilience within Pakistan's financial sector.

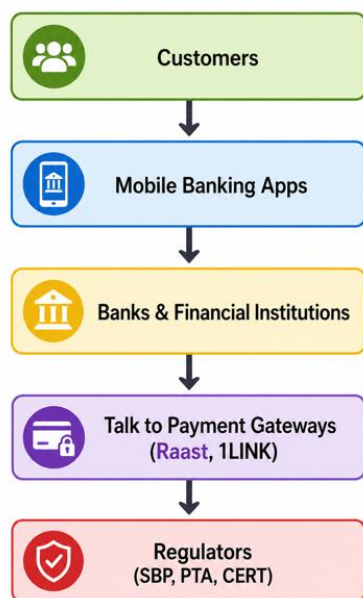


Fig.1 Digital financial ecosystem of Pakistan

Problem Statement

The swift adoption of digital technologies by Pakistan's financial institutions has enhanced banking efficiency, customer convenience, and financial inclusion (Raza et al., 2024). But, it has been a digital transformation that has also meant added exposure to cyber threats. Phishing, ransomware, malware, data breaches, and social engineering attacks pose increasingly significant threats to financial institutions, including the potential for financial losses, disruption of operations, damage to the institution's reputation, and destruction or compromising of customer data (Bello et al., 2025).

While regulatory bodies and organizations take steps to enhance cybersecurity practices, there are still obstacles to overcome such as lack of cybersecurity

awareness, a shortage of cybersecurity experts, outdated cybersecurity infrastructure, and regulatory compliance problems. Furthermore, more third-party vendors, cloud services, and fintech platforms are relying on these platforms, increasing vulnerabilities (Omole, 2026). In an era where the financial sector plays a crucial part in maintaining economic stability, it is imperative to address these cybersecurity challenges to ensure the resilience and security of financial operations.

Research Question

What are the major cybersecurity challenges facing Pakistan's financial sector, and how can financial institutions enhance their cybersecurity resilience to effectively mitigate emerging cyber threats?

II. LITERATURE REVIEW

A. Cybersecurity in Global Financial Institutions

Financial institutions are facing growing challenges from the increasing nature and sophistication of cyberattacks and have made cybersecurity a critical concern for their businesses around the world (Umoga et al., 2024). Banks and financial service providers are vulnerable targets, given the sensitive data they hold and the significant financial transactions they conduct. Cyber incidents have become a serious threat to financial stability, and could have an impact on payment systems, banking operations and financial markets, the International Monetary Fund (IMF) said (Brando et al., 2022). The World Bank also highlights the increased attack surface of financial institutions due to the digital transformation and the need for strong cyber security (Kudinova et al., 2025). As a result, financial firms are putting significant resources into cyber risk management, threat detection, and incident response technologies to build their cyber-resilience against new threats.

B. Digital Transformation and Emerging Cyber Threats in Pakistan

Internet banking, mobile banking, fintech services, and branchless banking solutions are the major measures that have witnessed a rapid digital transformation of the banking sector in Pakistan (Sikandar, 2025). The launch of the State Bank of Pakistan's (SBP) Raast payment system has further boosted digital transactions and financial inclusion

(Bokhari, 2022). These advancements have made things easier and faster, but have also led to greater reliance on digital systems and exposure to cyber risks.

Phishing and social engineering attacks are among the most frequent threats, where the cybercriminal communicates via deceptive emails, messages, and fake websites (Choi, 2023). Human error continues to be a large part of the successful attack, especially when dealing with users who may lack cyber security awareness. Cybercrime like malware and ransomware is also hazardous, causing disruption, information theft and loss of revenue. Financial firms are very vulnerable as they have services and data of high value (Edu, 2022).

The additional threat is data breach and insider threats which hamper cyber security efforts (Achor, 2022). The unauthorized use of customer information may lead to fraud, identity theft, reputational harm and regulatory fines. Furthermore, third-party vendors, financial technology partners and cloud service providers add to the supply chain risks (Banik, 2022). Financial institutions are subject to vulnerabilities in external systems, and attacks are becoming more frequent, making it increasingly important for them to have vendor risk management and continuous monitoring in place.

Table 1: Growth of digital banking users and digital transactions in Pakistan (2021-2024), highlighting the rise in mobile banking, internet banking, and digital payment channels.

Indicator	2021	2022	2023	2024
Mobile Banking Users (Millions)	11.9	13.5	16.0	18.6
Internet Banking Users (Millions)	6.9	8.2	11.0	13.8
Digital Transactions (Billions)	3.0	3.8	4.7	6.4

Sources: Compiled from State Bank of Pakistan (SBP) Payment Systems Reports and Annual Payment Systems Reports. Mobile banking users reached 16 million and internet banking users reached 11 million by the end of 2023. In FY2023, digital transactions grew from 4.7 billion to 6.4 billion in FY2024 (Associated Press of Pakistan, 2024).

C. Regulatory Frameworks and Cybersecurity Capacity

In response to these emerging cyber threats, regulators have developed cybersecurity frameworks to enhance cybersecurity resilience. SBP has published guidelines on cybersecurity for Governance, Risk Management and Incident Reporting (State Bank of Pakistan, 2026). Certain international standards, such as ISO/IEC 27001, offer a structured framework to manage information security risks and put in place effective controls (Culot et al., 2021). Likewise, the NIST Cybersecurity Framework is composed of five main functions (Identify, Protect, Detect, Respond, Recover) that enhance organizational resilience (Mahn, 2018). The Basel Committee on Banking Supervision further stresses the importance of the concepts of governance, business continuity planning and cyber-resilience as integral parts of operational risk management.

However, there is a shortage of cybersecurity experts in Pakistan. The increasing need for cybersecurity skills is outpacing the number of professionals available to fill the positions, making it harder for organizations to bolster their security systems and respond to cybersecurity incidents. In this regard, enhancement of cyber security education, professional certifications and awareness programs are important measures to enhance the cyber security resiliency of the financial sector in Pakistan.

III. RESEARCH METHODOLOGY

The design of this study is qualitative using secondary data analysis approach. To explore the issues of cybersecurity threats, regulatory environment and new risks in the financial sector of Pakistan, a qualitative approach has been adopted. The study uses secondary data sources such as literature review and authoritative reports rather than primary data collection methods like surveys or interviews to gain a deeper understanding of the subject.

The data were collected from trusted sources such as publications, cybersecurity guidelines of State Bank of Pakistan (SBP), World Bank, International Monetary Fund (IMF), ISO/IEC 27001 standard and the NIST Cybersecurity Framework. Banking cybersecurity-

related peer-reviewed journal articles and industry reports were also examined.

Thematic analysis was used for analysis of data, which aimed at showing the patterns and themes that occurred more than once. The analysis highlighted the threats in the cyber space, the regulatory measures, technological weaknesses and shortage of manpower, and categorized the major factors influencing the cybersecurity capability of financial institutions in Pakistan.

IV. FINDINGS

Theme 1: Rapid Digitalization Increases Attack Surface

The literature analysis shows that financial services' digitalization has considerably increased the attack surface of financial institutions. Adoption of internet, mobile banking applications, fintech services, cloud computing and digital payment systems have enhanced efficiency and financial inclusion, but have also heightened cyber security risks. The World Bank (2021) noted that the increasing interdependence of financial systems opens up new opportunities for hackers. Likewise, IMF states that the rise in usage of digital technologies has raised cyber risk exposure in the global financial sector (International Monetary Fund Secretary's Department, 2024). Digital banking platforms and Raast instant payment system have driven digital transactions and customer engagement in Pakistan. But with these advances come more complex financial infrastructure challenges. Aldasoro et al. (2020) state that the more digital institutions are integrated, the more vulnerabilities they have, especially if they use more digital channels in combination with third-party service providers. The results indicate that digital transformation is a driver of innovation and financial inclusion, but also introduces new cybersecurity issues that demand ongoing monitoring, risk analysis, and security technology investments. As such, cyber security should be a part of any digital transformation phase to guarantee the security and stability of Pakistan's financial system.

Theme 2: Phishing is the most prevalent threat.

All the reviewed literature agrees that one of the major cyber security threat that is faced by financial institutions is phishing. Phishing attacks rely on the

human element, using e-mail, text messages, telephone calls and fake Web sites to trick victims into disclosing personal information like their passwords, account numbers and banking information. Phishing is still one of the main ways that cybercriminals can access financial systems, according to the NIST Cybersecurity Framework (2023). World Economic Forum also notes that social engineering attacks are growing in number because they are based on the vulnerabilities of humans, not technology (Jurgens & Dal Cin, 2025). The rise in digital banking has created an increasingly big customer base in Pakistan that has fallen victim to phishing.

The State Bank of Pakistan has issued several warnings to financial institutions and their customers regarding communications that purport to be from banks and payment service providers (State Bank of Pakistan, 2026). In addition, the literature indicates that human error continues to be one of the major causes of cybersecurity breach incidents in the financial industry (World Bank, 2021). The results show that phishing attacks can be overcome if technological security measures are not applied. Instead, ongoing customer awareness campaigns, employee training and development initiatives, multi-factor authentication solutions, and proactive threat detection systems are needed to mitigate the risk of successful attacks.

Theme 3: Regulatory Improvements Are Strengthening Security

The results show that regulatory efforts have contributed significantly to boost the security of the financial sector in cyber space. The importance of cybersecurity to operational resilience and financial stability is becoming a priority for financial regulators around the world. The State Bank of Pakistan (SBP) has issued guidelines and cyber risk management frameworks for financial institutions in Pakistan, which mandate the creation of governance frameworks, risk management systems, and incident response procedures (State Bank of Pakistan, 2026). ISO/IEC 27001 and the NIST Cybersecurity Framework are international frameworks that offer a structured way of identifying, managing and reducing cybersecurity risks. Organizations with a risk-based cybersecurity program are more likely to identify, respond to, and recover from cyber incidents (NIST, 2023).

In the same way, the Basel Committee on Banking Supervision is stressing on cyber resilience with robust governance, business continuity planning and operational risk management (Gržeta et al., 2023). The literature indicates that the standards are correlated with the increase of an organization's readiness and fostering a culture of cybersecurity awareness. Moreover, regulatory supervision fosters the adoption of international best practices and investments in financial institutions' cybersecurity infrastructure. The results show that although cyber threats continue to grow and change, the regulatory environment is helping to increase security measures and resilience in the financial sector.

Theme 4: Lack of Cybersecurity Experts.

One recurring theme in the literature is the lack of qualified cybersecurity professionals. With the growth of the sophistication of cyber-attacks, organization's need individuals who are capable of carrying out threat analysis, handling security operations and responding to cyber incidents. But jobs in cybersecurity still outnumber the number of qualified candidates. According to the World Economic Forum Jurgens & Dal Cin (2025), the cybersecurity skills gap remains one of the top challenges to cyber-resilience around the world. Likewise, the World Bank (2021) highlights that developing countries have heightened problems in building cybersecurity capacity as a result of low educational resources and professional training opportunities.

Digital banking and fintech services are booming in Pakistan, creating a demand for cybersecurity experts, but many firms are facing difficulties in finding and keeping skilled workers. SBP has also recognized the importance of increasing investments in cyber security awareness, training and workforce development, to bolster the growing digital financial landscape (State Bank of Pakistan, 2026). The results show that a lack of staff can have a negative impact on an organization's ability to employ sophisticated security measures, detect threats, and react appropriately to a cyber-incident. To meet this challenge, it is essential to work together among the government, education, and industry to create cybersecurity education programs, certifications, and ongoing training efforts to build the nation's cybersecurity skills.

V. DISCUSSION

The results provide insights into the intricate dynamics between digital transformation and cybersecurity threat in the financial industry of Pakistan. While digital banking services offer unparalleled convenience for the customer and enhanced financial opportunities, they have also opened up more potential entry points for cyberattacks. This finding aligns with worldwide research which has found digitalisation to be one of the key drivers of the growth of cyber risk exposure in the financial industry.

The results also highlight the ongoing and persistent nature of phishing attacks. Past research indicates that technological security measures are not enough if human factors are not. Employee training, education of customers and awareness programs, and cybersecurity education are, therefore, critical to minimizing the impact of social engineering attacks.

The State Bank of Pakistan's regulations have been beneficial in enhancing the governance and management of cyber risks. Compliance of local regulations with internationally agreed upon standards like ISO 27001 and NIST Cybersecurity Framework reflects a step towards improved cybersecurity resilience. However, implementation of the effective type is still a challenge, especially for the institutions that lack in technical resources.

The analysis of international best practices shows that many advanced financial systems have put significant efforts into building their cybersecurity skills, improving their threat intelligence functions and ongoing security monitoring. Similar measures can be beneficial for the financial sector in Pakistan. To achieve long-term cyber resilience and ensure the trust in digital financial services, the cybersecurity skills shortage must be addressed and investments in contemporary security technologies must be ramped up.



Fig.2: Cyber Risk Management Cycle (NIST, 2023)

VI. RESULTS

According to the findings of this study, cybersecurity has emerged as a key issue for the financial industry in Pakistan, as digitalization and cyber threats are growing. Financial institutions are exposed to many threats, such as phishing attacks, ransomware attacks, data breaches, internal threats, and risks posed by third-party service providers.

The results indicate that phishing is still the top threat as it relies on human behavior and is continuing to impact customers and financial institutions. Another significant threat is ransomware attacks, as they can disrupt the operations and lead to significant financial losses. Data breaches may expose customer-sensitive data and harm the reputation of the organization, and insider threats may be associated with the unauthorized entry into the system and the misuse of sensitive information.

Table 2: Prominent Cybersecurity Challenges

Challenge	Impact	Risk Level
Phishing	Financial Fraud	High
Ransomware	Service Disruption	High
Data Breaches	Information Loss	High
Skill shortage	Unauthorized access	Medium

The results also indicate that the State bank of Pakistan's regulatory measures and implementation of global cybersecurity guidelines have enhanced cybersecurity governance. But obstacles like low cyber security skills and different degrees of cyber readiness within the sector persist in the sector's overall cyber resilience.

VII. CONCLUSIONS

The present study focused on analyzing key cyber security issues of Pakistan financial sector in the midst of digital transformation. The results show that digital banking, fintech services and electronic payment systems, whilst enhancing financial inclusion and the efficiency of financial operations, have also heightened risks of cyber-attacks. Risks are largely similar to those of other types of risks, such as phishing attacks, ransomware, data breaches, insider threats, third party vulnerabilities, etc. To safeguard financial assets, build customer trust, and ensure financial stability, it is crucial to have an effective cybersecurity governance framework supported by regulatory frameworks like SBP guidelines, ISO 27001, and NIST Cybersecurity Framework.

VIII. FUTURE WORK

Further studies on the new cybersecurity technologies should be conducted which can enhance the resilience of the financial system in Pakistan. Topics of interest include the use of Artificial Intelligence and Machine Learning in fraud detection, threat intelligence, and automated responses, and block chain-based security solutions. The risks of cybersecurity in fintech companies and digital payment service providers should be further explored. A quantitative study of the banks and financial institutions might be able to measure the level of cybersecurity maturity, analyze the current level of security controls, and suggest on-the-ground strategies for enhancing the sector's security.

REFERENCES

[1] International Monetary Fund. Secretary's Department. (2024). *International Monetary Fund Annual Report 2024 Financial Statements*. International Monetary Fund.

[2] Achor, O. (2022). *Data Security Strategies for Preventing Breaches Due to Insider Threats - ProQuest*. <https://search.proquest.com/openview/c3265b8c4a2bb65c2a42c9b35b93cfd0/1?pq-origsite=gscholar&cbl=18750&diss=y>

[3] Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). *Operational and cyber risks in the financial sector*. <https://www.bis.org/publ/work840.pdf>

[4] Associated Press of Pakistan. (2024, March 13). *Digital financial services experience significant growth in Q2-FY24*:

- SBP. Associated Press of Pakistan. <https://www.app.com.pk/business/digital-financial-services-experience-significant-growth-in-q2-fy24-sbp/>
- [5] Banik, S. D. (2022). *Third-Party Risk Management in the Financial Services Industry*. https://www.cs.ru.nl/masters-theses/2022/G_Keizer___Third-party_risk_management_in_the_financial_services_in_dustry.pdf
- [6] Bello, A., Wonuola, I., Izundu, A., & Izundu, J. (2025). Cybersecurity threats in the financial sector: Analyzing attack types, Vulnerabilities, and response mechanisms across geopolitical contexts (2015–2024). *International Journal of Science and Research Archive*, 16(1), 134–150. <https://doi.org/10.30574/ijrsra.2025.16.1.2007>
- [7] Bokhari, H. (2022). *Digital Financial Inclusion of the Informal Sector: The case of Raast Platform in Pakistan*. <https://doi.org/10.1145/3560107.3560136>
- [8] Brando, D., Kotidis, A., Kovner, A., Lee, M., & Schreft, S. L. (2022). Implications of Cyber Risk for Financial Stability. *Www.federalreserve.gov*. <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>
- [9] Choi, Y. (2023). Social Engineering Cyber Threats. *Journal of Global Awareness*, 4(2), 1–12. <https://doi.org/10.24073/jga/4/02/08>
- [10] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, 33(7), 76–105. <https://doi.org/10.1108/tqm-09-2020-0202>
- [11] Edu, A. S. (2022). Positioning big data analytics capabilities towards financial service agility. *Aslib Journal of Information Management, ahead-of-print(ahead-of-print)*. <https://doi.org/10.1108/ajim-08-2021-0240>
- [12] Gržeta, I., Žiković, S., & Tomas Žiković, I. (2023). Size matters: analyzing bank profitability and efficiency under the Basel III framework. *Financial Innovation*, 9(1). <https://doi.org/10.1186/s40854-022-00412-y>
- [13] Jurgens, J., & Dal Cin, P. (2025). Global Cybersecurity Outlook 2025. In *World Economic Forum*. World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
- [14] Kudinova, A., Maslii, O., Smokvina, V., & Tsyhanenko, K. (2025). THE IMPACT OF DIGITALIZATION ON THE FINANCIAL INSTITUTIONS' ECONOMIC SECURITY IN THE FACE OF GROWING CYBER THREATS. *Financial and Credit Activity Problems of Theory and Practice*, 4(63), 466–483. <https://doi.org/10.55643/fcaptop.4.63.2025.4790>
- [15] Mahn, A. (2018, October 23). *Identify, Protect, Detect, Respond and Recover: The NIST Cybersecurity Framework* | NIST. NIST. https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework?dtid=oblgzzz001087&utm_source=chatgpt.com
- [16] NIST. (2023). NIST Drafts Major Update to Its Widely Used Cybersecurity Framework. NIST. <https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework>
- [17] Omolere, O. (2026). *THIRD-PARTY CYBER RISK MANAGEMENT: AN AUDIT PERSPECTIVE Assessing How Organizations Audit Vendors, Cloud Providers, and Fintech Partners for Cybersecurity Compliance*.
- [18] Raza, M., Bilal, M. A., & Khan, A. B. (2024). FinTech Adoption and Sustainability Performance: The Role of Digital Financial Literacy and Financial Inclusion in Pakistan's Banking Sector. *Journal of Innovative Research in Management Sciences*, 5(4), 74–98. <https://doi.org/10.62270/jirms.v5i4.80>
- [19] Shrestha, S. (2025). *Branchless bnaking and financial inclusion; Reaching the unbanked and underbanked population*. Tucl.edu.np. <https://elibrary.tucl.edu.np/items/01f2fc3c-a27a-4587-a4d2-fd47d94945e8>
- [20] Sikandar, A. (2025). Digitalization and its Impact on Developing Economies: A Case Study of Pakistan's Banking Sector. *Intersect: The Stanford Journal of Science, Technology, and Society*, 18(2). <https://ojs.stanford.edu/ojs/index.php/intersect/article/view/3382>
- [21] State Bank of Pakistan. (2026). *State Bank of Pakistan Cyber Shield*. Sbp.org.pk. <https://www.sbp.org.pk/CRMD/2026/CL01.htm>
- [22] Umoga, J., Oluwademilade, E., Amoo, N. O. O., & Atadoga, N. A. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive*, 11(1), 1810–1817. <https://doi.org/10.30574/ijrsra.2024.11.1.0284>
- [23] World Bank. (2020). *Financial Sector's Cybersecurity*. Worldbank.org. <https://thedocs.worldbank.org/en/doc/361881595872293851-0130022020/render/CybersecDigestv5Jul2020FINAL.txt>