Cybersecurity Risk Governance in Pakistan's Fintech Sector: A Critical Assessment

Pakistan's Data-Driven Fintech Boom

Pakistan has a variety of intermediaries categorized within a financial system, which includes both bank and non-bank intermediaries. The former comprises commercial, Islamic, specialized, and microfinance banks, while the latter encompasses development finance institutions, non-bank financial companies, and insurance firms. In this environment, the banking sector is the most dominant in terms of asset size and systemic impact, accounting for almost 77% of the aggregate resources contributed by the financial sector and approximately 50% of GDP.

The management of such an ecosystem is primarily the responsibility of two apex authorities, namely the State Bank of Pakistan (SBP) and the Securities and Exchange Commission of Pakistan (SECP). The central bank is required to preserve financial stability under the SBP Act of 1956, which it exercises through the regulation of a wide variety of institutions and infrastructures, including microfinance banks (MFBs), development finance institutions (DFIs), exchange companies, payment service providers, and electronic money institutions (EMIs), among others.

As it aligns with global regulatory standards, the SBP has focused not merely on establishing resilience to systemic shocks but has also aimed to modernize financial intermediation through technology-enabled reforms, seeking to make it more inclusive and growth-inspiring.[1] However, in the latter half of the past decade, the country has experienced greater disruption in its financial sector than ever before—impelled by the high rate of penetration of digital financial technologies.

Dr. Azeema Usman
Assistant Manager (Research and Publications)
Saviours, Karachi

Credit scoring through artificial intelligence, biometric onboarding, instant microloans, QR-based merchant payments, and accessing remittances through apps have changed the parameters of access to finance. These platforms, including JazzCash, Easypaisa, SadaPay, Finja, and QisstPay, among others, now empower millions of Pakistanis to transact, borrow, or save with as little as a smartphone and a CNIC, effectively bypassing the frictions of traditional banking.

However, a deep-seated vulnerability is created due to the same innovations that are used to democratize finance. Every time we swipe, tap, or scan our face, it represents a gesture. The data translated into sensitive personal and monetary information is likely to be stored and processed by private operators working in the grey areas of regulation.

Table 1: Growth, Share, and Size of Pakistan's Financial Sector

Institutions	YoY Growth in Assets (%)			Percentage Share in Total Assets (%)			Assets as a Percentage of GDP (%)		
	2022	2023	2024	2022	2023	2024	2022	2023	2024
MFBs	29.4	2.4	38.5	1.6	1.3	1.5	1.0	0.8	1.0
DFIs	165.7	63.3	-15.5	1.9	4.0	2.8	1.9	4.2	2.8
NBFIs	26.7	34.5	80.0	5.5	5.8	8.9	3.6	3.4	5.8
Insurance	20.2	31.4	—	2.2	2.5	2.0*	1.2	1.3	1.2*
CDNS	-12.7	-6.2	1.5	7.3	5.4	4.6	4.5	3.3	3.0
Banks	19.1	29.5	15.8	77.0	78.5	77.2	47.8	48.4	50.0
Overall Sector	18.6	27.0	17.8	100	100	100	32.0	61.7	64.8

** Note: Insurance data is available up to September 2024.*
Sources: SBP, SECP, CDNS, PBS

As big data analytics emerges as the driving force behind financial inclusion, it simultaneously increases the risk of digital identity theft, algorithmic discrimination, API abuse, and cross-platform breaches.

Against this rapidly shifting backdrop, Pakistan's leap towards a "data-driven financial future" is part of an increasingly high-stakes security paradigm; hence, an invisible war can determine whether technological advancements will be an enabler of growth or a barrier to systemic fragility. [1]

The traditional financial system in Pakistan, previously troubled by organizational stasis, bureaucratic processes, and restricted geographical outreach, is being quickly overtaken by digitally based forms of financial services, which are now far more accessible and user-friendly than ever before. Today, millions of formerly underserved citizens can easily enjoy efficient digital payments, microcredits and savings products created by fintech programs. [2]

Fintech Landscape and Initiatives in Pakistan

The fintech landscape in the country is growing at an impressive rate, primarily driven by technological advancements, high smartphone penetration, and increasing internet access. Pakistan has a population of 240.5 million and a national target to further increase adult financial inclusion from its current rate of 64% to 75% by 2028, a figure in which fintechs will likely play a decisive role. The ecosystem has been further reinforced by regulatory efforts initiated by the State Bank of Pakistan (SBP), such as digital banking frameworks and sandbox environments, which have positioned the country as one of the most promising emerging markets for adopting fintech solutions.

The impetus towards achieving this is supported by Pakistan's digital infrastructure, comprising 193 million cellular subscribers and 143 million broadband connections, which provides the required scale for innovation. The SBP estimates that the digital payments market alone will grow to nearly USD 36 billion by 2025. In addition to payments, growth extends to digital lending, remittances, wealth management, and peer-to-peer financial services. [2] Currently, there are over 448 active fintech companies in Pakistan, of which Bazaar is ranked as the top fintech company in the country—evidence of the size and competitiveness of the industry. [3]

Since the early 2000s, fintech in Pakistan has steadily gained momentum, starting with mobile money services like Easypaisa, which revolutionized access to financial services through easy payments, deposits, withdrawals, and remittances. In 2012, JazzCash—a result of Mobilink (now Jazz) and the National Bank of Pakistan's collaboration—further extended digital transactions. [4] Several banks then rolled out their mobile banking services, following in the footsteps of these pioneers.

To accelerate adoption, the State Bank of Pakistan (SBP) and the government introduced several major initiatives, including the National Payment Strategy (NPSS), Micro Payment Gateway (MPG), and digital onboarding systems. The transaction volume of internet-based payments increased by 53 percent in 2018 compared to 2017, signifying rapid adoption by consumers in the late 2010s.

Fintech is also being implemented in microfinance institutions; one such institution is Telenor Microfinance Bank, which deployed the Khushhal Digital Platform in 2018 to enhance growth in digital services. Nowadays, there are over 422 fintech startups in Pakistan, and the success of fintech platforms like Abhi, NayaPay, and others reflects the growing consumer demand that is reshaping a financially inclusive digital ecosystem. [4]

Table 2: Leading Fintech Companies in Pakistan

Company	Description	Location	Founded	Private Funding Raised
Bazaar	A platform offering an operating system for general-purpose businesses	Karachi (Pakistan)	2020	USD 108M
Abhi	Online platform providing payday loans	Karachi (Pakistan)	2021	USD 19.1M
JazzCash	Mobile money service enabling online and offline payments	Islamabad (Pakistan)	2012	–
SadaPay	Digital bank offering individual banking solutions	Islamabad (Pakistan)	2018	USD 20M
Finja	Financial services provider for MSMEs, investors, and enterprises	Lahore (Pakistan)	2015	USD 25M

Source: Tracxn.(August 16, 2024). FinTech startups in Pakistan

Table 3: Cybersecurity Risks in Financial Technology

Category	Description	Example in Fintech	Potential Impact
User-Centric Attacks	Phishing, social engineering and, identity theft targeting customers' credentials and personal data	Fake SMS scams via JazzCash / EasyPaisa; synthetic identities on BNPL platforms	Account takeovers, fraudulent loans, loss of trust
Authentication & Data Risks	Weak or spoofed biometric systems, poor encryption, and data poisoning of AI/ML models	Deepfakes bypassing e-KYC; unencrypted CNIC storage; manipulated credit scoring inputs	Unauthorized access, algorithmic bias, compliance breaches
Infrastructure Vulnerabilities	Exploits in APIs, cloud misconfigurations, and unsecured storage	Poorly secured AWS buckets exposing fintech user data	Data breaches, reputational damage, systemic risk
Operational Disruptions	DDoS attacks, ransomware, and third-party vendor breaches undermining services	Fintech app downtime due to DDoS; ransomware crippling back-office servers	Service unavailability, financial losses, regulatory penalties
Human & Regulatory Gaps	Insider threats, poor cybersecurity awareness, and weak compliance culture	Employees leaking data; users sharing OTPs with fraudsters; lack of penetration testing	Legal liability, license suspension, investor distrust

Source: Author

Cybersecurity Risk: More Data, More Exposure

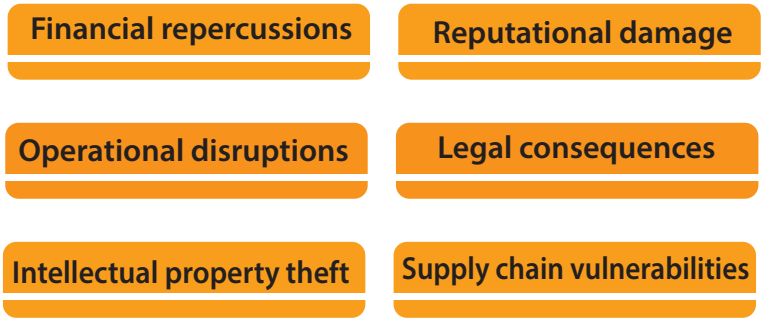
The consequences of a cyberattack on a fintech firm can be severe, ranging from financial loss to identity theft and damage to reputation. Worldwide patterns support this urgency: in 2024, 64% of financial institutions reported an increase in cyberattacks, and over 70% of market leaders anticipate a rise in financial crime risks in 2025 as technological change accelerates. [5,6]

Currently, Pakistan lacks a comprehensive data protection system, which creates considerable loopholes in the protection of financial data. The pre-existing Electronic Transactions Ordinance (2002) and Prevention of Electronic Crimes Act (PECA, 2016) provide limited action against the misuse of sensitive data. It is this regulatory vacuum that is especially troubling to fintech startups, which often conduct business in experimental sandboxes and rely heavily on third-party cloud-based infrastructure systems and open Application Programming Interfaces (APIs), which have been shown to offer attractive points of entry to cybercriminals. [5]

The cybersecurity risk in Pakistan's financial industry has escalated to a systemic challenge due to several factors, such as the ubiquity of digital technology among institutions and consumers, the entrenchment of interconnected financial platforms, the intense dependence on data, and the complexity of cyber-attacks. Over time, financial institutions are increasingly adopting emerging technologies, and their dependence on external service providers, such as cloud operators and fintech platforms, further complicates risk management, as these entities frequently fall beyond the direct purview of financial regulators.

The State Bank of Pakistan, through its first survey—the Systems Risk Survey—reported that risks related to cybersecurity are among the ten key risks to the financial system. Although the legal framework has been strengthened through the enactment of the PECA Act (2016), which formulated a legal process for investigation and prosecution, implementation has been fragmented. The National Response Center for Cyber Crime (NR3C), established under the Federal Investigation Agency (FIA), has been mandated to combat technology-related crimes at the institutional level. [7]

Figure 1: Consequences of Cyber Attacks in FinTech



Source: https://www.apriorit.com/dev-blog/cybersecurity-risks-in-fintech-software

Table 4: Major Cybersecurity Incidents in Pakistan's Financial & Fintech Sector

#	Institution / Sector	Date	Incident	Details & Impact
1	**Multiple Banks / Payment Cards**	Oct 2018	Coordinated ATM & payment network breach	Information of ~20000 debit/credit cards of 22 banks (HBL, UBL and BankIslami) was exposed to the dark web. There were fraudulent ATM withdrawals to the value of ~PKR 26 million which resulted in the temporary blocking of international transactions.[10]
2	**National Bank of Pakistan (NBP)**	Oct 2021	Malware attack disrupting services	ATM and online banking systems went offline due to boot-sequence corruption. No confirmed data loss but critical disruption across national banking operations was reported.[11]
3	**Securities & Exchange Commission of Pakistan (SECP)**	Aug 2022	Regulatory database breach	Personal sensitive information of directors of the companies (CNICs address emails) were leaked. Claims of an internal cover-up led to the demand of an independent investigation.[12]
4	**National Institutional Facilitation Technologies (NIFT)**	Jun 2023	Cyber breach of cheque clearing system	Data centers in Karachi and Islamabad were compromised forcing a switch to manual cheque clearing. This caused significant nationwide delays and disruptions across all banks.[13]
5	**BankIslami Pakistan & Meezan Bank**	2022 -23	Fraudulent SWIFT transfer & phishing scams	Hackers stole USD 6 million through fraudulent SWIFT transactions at BankIslami and Meezan Bank customers targeted by SMS phishing campaigns leading to widespread credential theft.[14]
6	**PKCERT / National Advisory**	May 2025	Global credential breach	Around 184 million credentials (emails logins passwords) were exposed globally including Pakistani banking government and technology users PKCERT issued urgent advisories for password resets and stronger security practices.[15]

Source: Author

Case Studies: Where the System Broke

A study conducted by Kaspersky reported a 114% increase in banking and financial malware attacks over the previous year, targeting digital financial activity and compromising both personal and organizational security. One of the trends that appears particularly threatening is the increased rate of cyberattacks on smartphones, which is likely to remain the focus of financial crimes through 2025.[8] The PwC survey also confirmed the susceptibility of the Pakistani financial industry.

Ransomware, phishing, and Distributed Denial of Service (DDoS) attacks have become primary threats to many banks, which are often challenged by conventional defenses. The rapid increase in mobile banking and online payments has significantly increased the amount of sensitive data circulating online, making financial institutions highly attractive targets for hackers.[9] The tension between financial technology and security in Pakistan is increasingly evident in several reported cases.

Regulatory Readiness: Is Policy Catching Up?

With the advent of the fintech industry in Pakistan, characterized by high levels of digitization, the regulatory environment has struggled to keep pace with dynamic threats. Despite the numerous cybersecurity guidelines issued over the past few years, workarounds are still necessary for implementation, inter-agency cooperation, and readiness for new risks, such as AI-based fraud, deepfakes, and cross-border internet crime.

Cybersecurity oversight continues to be organically dispersed across various organizations, including the State Bank of Pakistan (SBP), Securities and Exchange Commission of Pakistan (SECP), Pakistan Telecommunication Authority (PTA), and the Ministry of IT & Telecommunication (MoITT). Even though these regulators have announced frameworks specific to their industrial environments, such as the Cybersecurity Framework for Banks (2020) or the SECP Guidelines for NBFCs (2021), the absence of a uniform cybersecurity regulation nonetheless leaves fintechs operating in regulatory gray zones.

Table 5: Regulatory Landscape

Regulator	Regulation/Framework	Key Focus
SBP	EFT Regulations, Cybersecurity Guidelines	Payments, Banks, DFSPs
SBP	Digital Banks Framework (2022)	Digital-only banks
SECP	Cybersecurity Framework for NBFCs	Fintechs, E-wallets
SECP	Cloud Guidelines (2023)	Data sovereignty, Cloud risk
MoITT	Personal Data Protection Bill	Data privacy, User rights
PTA	Telecom Cybersecurity Framework	Mobile wallets/infra
GoP	National Cybersecurity Policy (2021)	Critical financial infrastructure

Source: Author

Working in the gray areas of hybrid peer-to-peer lending, crowdfunding, and blockchain has become especially uncertain. These weaknesses are further aggravated by the Draft Personal Data Protection Bill (2023), introduced several years late; unless enacted, fintechs will not be under a binding legal obligation to inform users about breaches or uphold data sovereignty, exposing millions of users to the risk of their data being misused with no definite solution in law.

Table 6: Identified Gap

Regulatory Element	Current Status in Pakistan	Global Best Practice
Unified Data Protection Law	Draft pending approval	GDPR (EU), DPDPA (India)
Mandatory Breach Notification	Not legally enforced	Within 72 hours (GDPR)
Fintech-specific Cyber Oversight	Fragmented, sector-based	Unified fintech regulators (e.g., MAS in Singapore)
Real-Time Monitoring	Limited SOCs and threat intelligence sharing	Federated CERT model (US, EU)
Cloud Risk Management Standards	Guidelines only for NBFCs	Mandated cloud audit trails and encryption (Singapore, UK)

Source: Author

In the Pakistani fintech sector, compliance with cybersecurity is typically reactive rather than systematic. A third-party audit is conducted by many firms only when necessary to raise funds or renew licenses, but it is not a continuous security measure. Although the State Bank of Pakistan has begun experimenting with RegTech-based supervision, its impact is currently limited to scheduled banks, where a general environment of under-monitoring fintech persists.

In comparison, other regulatory frameworks on privacy principles, such as the EU's General Data Protection Regulation (GDPR), Singapore's MAS Technology Risk Management Guidelines, and India's Digital Personal Data Protection Act (2023), are significantly more stringent. The lack of incident reporting requirements, as well as centralized registries of breaches, also contributes to the problem, leaving users in the dark. Pakistan is severely lagging in three vital aspects:

- **Data portability and user consent procedures:** There is no binding procedure specifying how users can maintain control over their financial data in terms of collection, sharing, or repurposing.
- **Cross-border incident disclosure mechanisms:** No rules exist for prompt reporting, especially when cyberattacks exploit international networks or cloud infrastructures.
- **Cyber insurance requirements for fintech companies:** There is no obligation for companies to have cyber insurance, thus exposing both businesses and customers to financial risks.

Policy Recommendations

- Pass and implement the Personal Data Protection Law to establish enforceable guidelines on data privacy, user consent, and breach notification.
- Broaden SBP and SECP regulatory scrutiny to all categories of systematic fintech, especially startups and those not currently under regulatory purview, to ensure standard conformity.
- Establish a centralized Fintech Cybersecurity Cell within the National CERT to enable real-time incident reporting and sharing, intelligence exchange, and coordinated responses.

Although Pakistan has significantly advanced its position in the region in terms of cybersecurity regulation, the current approach of the state is more reactive than proactive. The governance framework for fintech should be transformed into a proactive, risk-oriented system, rooted in strong data protection regulations, predictive supervision, and healthy cross-sectoral alignment.

Reference

[1] *Financial Stability Review – 2024 State Bank of Pakistan https://www.sbp.org.pk/FSR/2024/Overview.pdf https://www.sbp.org.pk/FSR/2024/index.htm*

[2] *Invest2Innovate (2025), The Fintech Landscape in Pakistan: Progress and Potential https://invest2innovate.com/the-fintech-landscape-in-pakistan-progress-and-potential/*

[3] *https://tracxn.com/d/explore/fintech-startups-in-pakistan/__OOMGzleyZYPyvEWpfn5a944aEy78_IJ8i3yxi2iu-K8#top-companies*

[4] *Qaiser, H., & Fahad, M. (2024). Fintech in Pakistan: current landscape, challenges, and global insights. Bulletin of Business and Economics (BBE), 13(3), 48-53. https://bbejournal.com/BBE/article/view/953/1015*

[5] *Neontri. (2025, August 9). Fintech security: How to resist cyber attacks in the digital era. https://neontri.com/blog/fintech-security/#:~:text=This%20trend%20reflects%20a%20sad,should%20keep%20on%20their%20radar.*

[6] *Siddiqui, S. A., & Ali, M. (2023). Emerging Trends and Challenges in Cybersecurity for Fintech. In Cybersecurity in the FinTech Era(pp 1–20). IGI Global. https://www.igi-global.com/chapter/emerging-trends-and-challenges-of-cyber-security-in-fintech/351207*

[7] *State Bank of Pakistan. (2017). Financial Stability Review 2017: Box 6.1 – Emerging challenge of cyber attacks: Implications for the financial sector. Retrieved August 9, 2025 https://www.sbp.org.pk/fsr/2017/boxes/Box-6.1.pdf*

[8] *Rizvi, J. (2024, November 19). Cyber threats in Pakistan's finance sector surge by 114pc in 2024: Report. The News International https://www.thenews.com.pk/print/1252393-cyber-threats-in-pakistan-s-finance-sector-surge-by-114pc-in-2024-report?utm_source*

[9] *Iqbal, S. (2024, November 26). 90% of bankers see cybercrimes as the biggest threat. Dawn https://www.dawn.com/news/1874847*

[10] *The Times of India+4Daily Lead Pakistan+4Asia Times+4Reddit*

[11] *https://pakobserver.net/cyber-attack-on-nbp/?utm_source*

[12] *https://www.csidb.net/csidb/incidents/5172a73d-59d6-46a3-8148-876b2ea3cfe6/?utm_source*

[13] *https://www.dawn.com/news/1913465/over-180m-users-passwords-login-credentials-stolen-in-massive-data-breach-says-national-cyber-security-body?utm_source*

[14] *https://tribune.com.pk/story/2423324/cybersecurity-breach-at-nift-puts-national-security-at-risk-1?utm_source*

[15] *https://www.idealsols.com/cybersecurity-vulnerabilities-in-pakistani-banking-systems/*

About Author: *The writer holds a PhD in Economics and has authored over 23 published articles and presented more than 15 research papers at international and national conferences. With eight years of diverse research experience across multiple organizations, she currently serves as Assistant Manager, Research and Publication, at Saviours.*