Cyber Risk in Financial Technologies (FinTech) and Customer Trust

Dr. S. Ramakrishnan
Associate Professor
Department of Banking & Finance
Government Arts College, Coimbatore, Tamil Nadu, India
Email: *s.ramakrishnan.bf@gaccom.edu.in*

Ms. Ritu Banerjee
Assistant Professor
Department of Management Studies
Ramakrishna Mission Vivekananda Centenary College,
Kolkata, West Bengal, India
Email: *ritu.banerjee1989@gmail.com*

ABSTRACT

Financial Technologies (FinTech) have revolutionized financial services by offering innovative solutions such as digital payments, peer-to-peer lending, robo-advisory, and blockchain-based platforms. However, the rapid adoption of FinTech has amplified cyber risks, including data breaches, fraudulent transactions, and platform vulnerabilities. Customer trust is crucial for FinTech adoption, as users must feel confident in the security, privacy, and reliability of these services. This paper explores the relationship between cyber risk in FinTech and customer trust. It examines risk sources, trust determinants, regulatory frameworks, and mitigation strategies. A conceptual framework is proposed to demonstrate how cyber risk management, transparency, and compliance collectively influence customer trust. The paper emphasizes that robust cybersecurity and proactive risk communication are essential for sustaining user confidence in FinTech ecosystems.

KEYWORDS: *FinTech, Cyber Risk, Customer Trust, Digital Payments, Regulatory Compliance*

Page 29-35 © MANTECH PUBLICATIONS 2025. All Rights Reserved

INTRODUCTION

FinTech has transformed traditional financial services by leveraging digital technologies to provide faster, more accessible, and personalized financial solutions. Services such as mobile wallets, online lending, digital banking, and blockchain platforms are increasingly integrated into daily life.

However, FinTech platforms face heightened cyber risks due to the sensitivity of financial data, high-value transactions, and reliance on complex software architectures. Customer trust is a central driver of FinTech adoption; a perceived lapse in security can lead to customer attrition, reputational damage, and regulatory scrutiny.

This paper investigates the interplay between cyber risk and customer trust in FinTech. It examines the sources of cyber risk, trust determinants, and regulatory measures. The study proposes a framework for managing cyber risk in ways that sustain and enhance customer trust.

Objectives of the paper:

1. To identify key cyber risks in FinTech platforms.
2. To analyze factors influencing customer trust.
3. To examine regulatory and governance frameworks.
4. To propose a trust-focused risk management framework.

2. CYBER RISKS IN FINTECH

2.1 Data Breaches and Privacy Violations

FinTech platforms collect sensitive personal and financial information. Unauthorized access or breaches can compromise user accounts, leading to identity theft and financial loss.

2.2 Fraud and Payment Risks

Cybercriminals exploit vulnerabilities to conduct fraudulent transactions, phishing attacks, and synthetic identity fraud.

2.3 Platform and Software Vulnerabilities

FinTech platforms rely on APIs, cloud infrastructure, and third-party integrations. Vulnerabilities in these components may be exploited for attacks.

Page 29-35 © MANTECH PUBLICATIONS 2025. All Rights Reserved

2.4 Insider Threats

Employees or administrators with privileged access can inadvertently or maliciously cause data leakage or system disruption.

Table 1: Key Cyber Risks in FinTech Platforms

Risk Type	Description	Potential Impact on Customers
Data Breach	Unauthorized access to personal/financial data	Loss of privacy, financial loss
Fraud	Phishing, payment fraud, account takeover	Financial loss, reduced trust
System Vulnerabilities	API or software exploits	Service disruption, transaction failure
Insider Threats	Malicious or negligent employee actions	Data misuse, reputational harm

3. CUSTOMER TRUST IN FINTECH

3.1 Dimensions of Trust

Customer trust in FinTech involves:

- **Security trust:** Confidence in protection against cyber threats
- **Reliability trust:** Assurance of consistent service availability
- **Transparency trust:** Clear communication on data usage and risk management
- **Regulatory trust:** Assurance that the platform complies with relevant laws

3.2 Trust and Adoption

Research shows that perceived security and transparency strongly influence user willingness to adopt and continue using FinTech services.

3.3 Trust Erosion

Even minor security incidents can disproportionately damage trust due to the financial and personal stakes involved.

Page 29-35 © MANTECH PUBLICATIONS 2025. All Rights Reserved

4. REGULATORY AND GOVERNANCE FRAMEWORKS

4.1 Data Protection Regulations

Laws such as GDPR (EU), Personal Data Protection Act (India), and PCI DSS standards guide secure handling of sensitive financial data.

4.2 Cybersecurity Guidelines

Central banks and financial regulators provide cybersecurity frameworks for FinTech platforms, covering risk assessments, incident reporting, and third-party oversight.

4.3 Compliance and Assurance

Regulatory compliance signals organizational accountability, fostering user confidence in secure digital transactions.

5. CYBER RISK MITIGATION STRATEGIES

5.1 Technical Controls

- Multi-factor authentication (MFA)
- Encryption of sensitive data
- Secure APIs and software vulnerability management
- Anomaly detection and real-time fraud monitoring

5.2 Organizational Controls

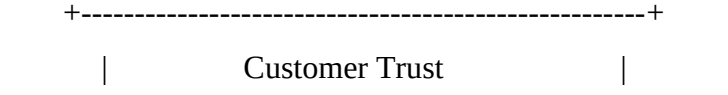
- Employee training on security best practices
- Governance frameworks for third-party risk
- Incident response and recovery plans

5.3 Trust-Building Measures

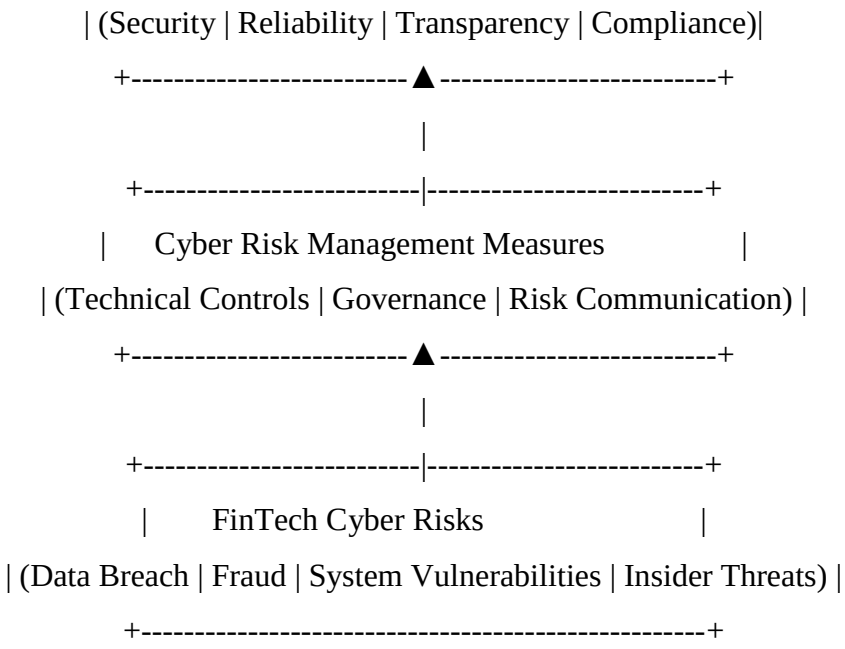
- Transparent risk communication
- User consent and privacy dashboards
- Third-party audits and security certifications

5. CONCEPTUAL FRAMEWORK: CYBER RISK MANAGEMENT AND CUSTOMER TRUST

Figure 1: FinTech Cyber Risk–Trust Framework (2D Representation)



Page 29-35 © MANTECH PUBLICATIONS 2025. All Rights Reserved



This framework demonstrates how proactive risk management and transparent communication can maintain and enhance customer trust.

7. SECTORAL PERSPECTIVES

7.1 Digital Payments

Mobile wallets and payment gateways face high exposure to fraud and phishing. Customer trust depends on secure transaction processing and incident transparency.

7.2 Lending and Investment Platforms

P2P lending and robo-advisory platforms must protect financial data and maintain algorithmic integrity to sustain trust.

7.3 Blockchain and Cryptocurrency

While blockchain promises security, wallet and exchange vulnerabilities can undermine trust if user funds are compromised.

8. CHALLENGES IN BALANCING RISK AND TRUST

- Rapid technological change creates new attack vectors
- Regulatory lag in emerging FinTech segments
- Balancing usability with robust security measures

Page 29-35 © MANTECH PUBLICATIONS 2025. All Rights Reserved

- Building trust across culturally diverse customer bases

9. FUTURE DIRECTIONS

Emerging strategies include:

- AI-driven threat detection and adaptive security
- Real-time customer communication on risk status
- Blockchain-enabled identity and transaction verification
- Trust dashboards showing security posture and compliance

10. CONCLUSION

Cyber risks in FinTech platforms pose significant challenges to customer trust, which is a critical determinant of adoption and engagement. Technical safeguards, regulatory compliance, and transparent communication collectively shape trust perceptions. This paper highlights that cybersecurity measures alone are insufficient; organizations must integrate proactive risk management, user-centric transparency, and governance practices to sustain confidence. By prioritizing trust alongside innovation, FinTech platforms can ensure secure, resilient, and user-friendly digital financial ecosystems.

REFERENCES

1. Arner, D. W., Barberis, J., & Buckley, R. P. *FinTech, RegTech, and the Reconceptualization of Financial Regulation*. Northwestern Journal of International Law & Business, 2017, pp. 371–413.
2. Kshetri, N. *1 Cybersecurity Issues in FinTech: Threats, Risks, and Regulatory Challenges*. Computer, Vol. 51, No. 11, 2018, pp. 44–52.
3. ENISA. *Cybersecurity in the Financial Sector*. European Union Agency for Cybersecurity, 2019, pp. 15–40.
4. PwC. *Global FinTech Report: Securing Trust in Digital Financial Services*, 2020, pp. 8–34.
5. OECD. *Digital Security Risk Management for FinTech Ecosystems*, 2021, pp. 21–56.
6. Floridi, L. *Trust and Digital Finance*. Philosophy & Technology, Vol. 33, No. 4, 2020, pp. 533–547.
7. PCI Security Standards Council. *Payment Card Industry Data Security Standard (PCI DSS)*, 2022, pp. 5–38.

Page 29-35 © MANTECH PUBLICATIONS 2025. All Rights Reserved

8. Basel Committee on Banking Supervision. *Cyber-resilience: Principles for the Financial Sector*, 2021, pp. 12–46.
9. Deloitte. *Trust and Security in FinTech: Building Customer Confidence*, 2022, pp. 19–48.

Page 29-35 © MANTECH PUBLICATIONS 2025. All Rights Reserved