pwc

Unified Fintech Forum
POWERING RESPONSIBLE FINTECH

FinSec: An emerging equation between FinTech and cybersecurity

Table of contents

Foreword 04

Message from PwC 05

01 Introduction 06

02 Revolution in the financial sector: Securing the future 08

03 The FinTech firewall – Current and the emerging challenges 11

04 Technological advancements entailing cybersecurity 15

05 Securing the future of FinTech – The security playbook 16

06 Regulatory developments in BFSI and its impact 18

07 An overview of FinTech cyber breaches 20

08 Conclusion 22

Foreword

Jatinder Handoo
CEO, UFF

As technology continues to redefine the limits of transparency, speed and inclusion, the financial landscape is undergoing a paradigm shift. At the Unified Fintech Forum (UFF), we have personally witnessed the remarkable progress made by India's FinTech sector, which has been driven by innovation, supportive government policies and a spirit of entrepreneurship.

India is currently the third-largest FinTech ecosystem in the world,[1] providing digital payments, lending, neobanking and blockchain solutions that are revolutionising access to finance. The rate of adoption is significant, with over 650 million smartphone[2] users and hundreds of millions of individuals participating in digital financial services ecosystem.[3] More importantly, these advancements are bridging the credit gap and democratising financial services for millions of individuals who were previously unserved.

Nevertheless, this expansion also imposes a significant burden on all stakeholders. The convergence of finance and technology has introduced new threat vectors – cyber fraud, data intrusions and targeted attacks. Robust cybersecurity is no longer an option. It is the foundation for sustainable growth, as recent survey findings and global case studies discussed in this report underscore.

I strongly encourage FinTech leaders, customers, policymakers, innovators and researchers to work in close collaboration. India can establish itself as a global FinTech juggernaut by establishing secure, resilient systems, and cultivating a culture of trust and compliance. Please join me in ensuring that the digital revolution is not only inclusive but also secure, safeguarding the very foundation of our financial system, institutions and consumers.

This is a timely report that sheds light on both the main challenges and actionable solutions. I commend the PwC and UFF teams for their comprehensive analysis and hope that it will enable readers to fortify and secure the future of FinTech in India.

---

1 https://cfo.economictimes.indiatimes.com/news/indian-fintech-sector-3rd-largest-globally-funded-ecosystem-raises-1-9-bn-in-2024/117192606#:~:text=News-,Indian%20fintech%20sector%203rd%20largest%20globally%2Dfunded%20ecosystem%2C%20raises%20%241.9,a%20report%20showed%20on%20Monday

2 https://blogs.idc.com/2024/10/09/from-discard-to-demand-the-growing-popularity-of-used-smartphones/#:~:text=There%20are%20approximately%20650%20million,from%20brands%20to%20component%20makers

3 https://www.omfif.org/2023/11/indias-digital-leap-in-financial-inclusion/?utm_source=chatgpt.com

Message from PwC

Sundareshwar Krishnamurthy
Partner, India Cyber leader
PwC India

With each passing day, the world is becoming more digital. At the centre of this digital evolution stand FinTechs, whose growth has been one of the most significant developments in the financial sector in the past few years. However, with increased digital adoption, cybersecurity becomes imperative and central to business resilience.

In this digital era, FinTech and cybersecurity are inextricably linked, with one preserving the integrity and the other defining the sustainability of our modern financial system. This relationship is both permanent and codependent in nature as both fields have their roots in technology.

Emerging technologies are opening new avenues and areas that can be exploited by threat actors. Blockchain and artificial intelligence (AI)-driven payments are not just making financial services more efficient and accessible but also giving rise to new vulnerabilities. The government has been laying increasing emphasis on securing the digital space for FinTechs. Maintaining a robust security posture is critical from a regulatory as well as a business viewpoint.

Moreover, customers are the most important stakeholders, and their interests lie at the heart of the FinTech–cybersecurity equation. Building customer trust is the most fundamental element for any business, and therefore protecting customer data becomes non-negotiable.

We believe that this linkage between FinTech and cybersecurity would continue to grow and become stronger. It will be paramount in driving innovation, safety, trust and resilience across the financial ecosystem.

Our report delves into this relationship by highlighting the FinTech landscape, current and emerging cybersecurity challenges, key recommendations, and the evolving regulatory environment for financial institutions.

I would like to thank my colleagues from UFF for contributing their valuable insights to this report.

01

Introduction

The FinTech sector stands at the forefront of India's digital financial revolution. In the same way that smartphones redefined communication, FinTech is changing how financial services are accessed, delivered and experienced. Home to the world's third-largest FinTech ecosystem,[4] India has witnessed a tremendous rise in digital payments, neobanking, lending platforms, and blockchain innovation. Widespread internet penetration, a vibrant startup culture, regulatory support, and a young, tech-savvy population are fuelling the ongoing transformation. The synergy between finance and technology is not just enhancing existing models but also creating entirely new financial paradigms. These developments are driving India's financial sector into an era of higher inclusion, efficiency and global competitiveness.

Observing the evolution of banking is a truly remarkable experience. The idea that 'banking is necessary, but banks are not' captures the essence of this transformation. Financial services are increasingly becoming more digital, decentralised and accessible, without relying on traditional banks.

With rapid progress in FinTech, banking is becoming more modern. The sector is disrupting traditional banking models and improving user experience and efficiency for financial organisations.

Over the past decade, India's FinTech industry has undergone a rapid metamorphosis. Peer-to-peer lending platforms, mobile payment systems, digital wallets and robotic advisors have fundamentally transformed the financial landscape. India's digital prowess is evident, with the smartphone user base estimated to be over 1.1 billion and internet users, around 900+ million in 2025.[5] Government initiatives supporting a cashless economy, along with the introduction of the Unified Payments Interface (UPI) system, have been a major game changer. As of May 2025, UPI witnessed a record high of 18.68 billion transactions, with a total value of INR 25.14 lakh crore.[6]

At the same time, the global FinTech market, which was valued at more than USD 340 billion in 2024, is projected to grow at a double-digit compound annual growth rate (CAGR) till at least 2032.[7] This rapid expansion is being driven by advancements in digital infrastructure, increasing financial inclusion, and widespread adoption of innovative financial services across developed and developing economies.

India is emerging as a major player in the global FinTech landscape, showcasing commendable growth and innovation in the past few years. India has about 10,200 FinTech companies and currently holds the third-highest number globally, trailing only behind the US (~31,500) and the UK (~12,500). Notably, India outperforms several other wealthier nations such as Germany, Canada, France and Australia in terms of FinTech scale-ups. This underlines the fact that factors apart from GDP per capita – such as access to funding, government support and startup-friendly policies – play a pivotal role in fostering innovation in the FinTech sector.[8]

---

4 https://www.business-standard.com/finance/personal-finance/india-home-to-26-fintech-unicorns-with-a-combined-market-value-of-90-bn-124090300565_1.html

5 Inc42, State of India FinTech Report 2024

6 https://www.npci.org.in/what-we-do/upi/product-statistics

7 https://www.fortunebusinessinsights.com/FinTech-market-108641

8 https://www.business-standard.com/finance/personal-finance/india-home-to-26-fintech-unicorns-with-a-combined-market-value-of-90-bn-124090300565_1.html

9 https://www.fortuneindia.com/economy/indias-FinTech-market-projected-to-grow-to-over-400-billion-by-fy29-says-fm-nirmala-sitharaman/124175#gfintehc%20oogle_vignette

According to Finance Minister Nirmala Sitharaman, the Indian FinTech market is expected to grow by USD 400 billion by the fiscal year 2028–29. This growth corresponds to an anticipated annual growth rate of ~30%, reflecting strong momentum in digital payments, lending, InsurTech and other FinTech services. As India continues to focus on financial inclusion and digital transformation, its FinTech ecosystem is poised to become one of the most dynamic and influential in the world.[9]

In the era of FinTechs, cybersecurity is enabling FinTech companies to secure digital finance by using encryption, implementing fraud detection to safeguard transactions and data, and building trust in innovative financial technologies across global platforms.

02

Revolution in the financial sector: Securing the future

2.1

FinTech: India's emerging economic powerhouse

India's FinTech sector has observed remarkable growth in the past few years, propelled by increased smartphone adoption and a strong digital payments ecosystem. The industry's leading players are trying to harness emerging technologies such as AI and application programming interface (API)-based platforms to drive financial inclusion and deliver cutting-edge solutions. Progressive government policies and a vibrant startup landscape are supporting the momentum, making India one of the global hubs for financial technology innovation and development.

Technology is acting as a key enabler for FinTechs, with cloud computing providing scalability and cost efficiency, APIs driving open banking and integration, AI and machine learning (ML) enhancing personalisation and fraud detection, blockchain ensuring transparency and decentralisation, and data analytics supporting risk modelling and customer insights.

India's FinTech sector plays a vital role in making financial services accessible to millions of underbanked and unbanked individuals. The sector has the potential to evolve into a USD 1 trillion market by 2030.[10]

A key indicator of India's success is its FinTech adoption rate of 87%, which is much higher than the global average (67%). This progress has been driven by a collaborative ecosystem involving government initiatives, private innovation, financial institutions and public participation.[11]

Union Finance Minister Nirmala Sitharaman highlighted the role of banks and FinTech firms in India's achievement of 80% financial inclusion in just six years – a milestone that would typically take five decades.

This digital revolution has been made possible by the widespread adoption of UPI, which now has approximately 35 crore (350 million) active users and is operational in seven countries. UPI facilitates nearly half of all real-time digital transactions globally, which solidifies India's leadership in the digital payment space.[12]

Indian FinTechs are gaining popularity across the globe, with more and more nations wanting to collaborate with India and adopt its model. This sector is not just transforming India's financial landscape but also establishing new international standards for innovation, scale and inclusion.

10 PwC, Beyond the cloud: Navigating FinTech cyber threats and fortifying defences report

11 https://www.pib.gov.in/PressReleasePage.aspx?PRID=2137549

12 https://www.pib.gov.in/PressReleasePage.aspx?PRID=2137549

2.2

The growing cyber threat landscape

The FinTech era has seen the emergence of new types of fraud, with digital arrest scams, KYC fraud, UPI frauds, task-based job scams, electricity bill scams, lottery frauds, etc., becoming increasingly common. It has opened the door to new cybersecurity challenges that pose serious threats to financial institutions and their customers.

From a broader perspective, the world of FinTech is driven by three key factors – technological advancements, regulatory landscape and shifting consumer preferences. The global FinTech market is poised to grow with advancements and innovation in areas such as payments, digital banking and investment solutions. However, challenges associated with managing regulations and compliance frameworks, risks from cybersecurity threats, and limitations posed by outdated infrastructure can be impediments for the industry.

Cybersecurity breaches are already causing organisations worldwide significant losses, with the average cost of a global data breach exceeding USD 3 million. As per our 2025 Global Digital Trust Insights report, over a quarter of senior executives believe that their most damaging data breach in the past three years cost their organisation at least USD 1 million.

Geopolitical tensions are further impacting the cybersecurity posture of large as well as small financial institutions. Traditional geopolitical conflicts are gradually evolving into information-based warfare. This is also pointing towards the rising cyber threats to the financial infrastructure of the affected regions.

As a fundamental pillar of national economies, financial systems continue to remain the prime targets for cyberattacks, espionage as well as disruption. Protecting these institutions from external threats is no longer optional but essential. Strengthening cybersecurity measures, enhancing threat intelligence, and fostering global cooperation are crucial to safeguard financial stability in an era where cyber warfare is an extension of geopolitical conflict.

Due to the increasing number of FinTechs, attack surfaces are also multiplying. Therefore, security is no longer an option – it is the foundation of a robust ecosystem.

2.3

FinTech market forecast: An overview of key FinTech sub-sectors

As the FinTech sector continues its upward trajectory, several key FinTech sub-sectors are expected to maintain the growth momentum. The table below outlines these sub-sectors and provides projections for their total addressable market by 2030.

LendingTech

Aims to make lending more efficient, accessible and inclusive by improving credit assessment processes, automating loan approvals and facilitating faster disbursement of funds. Often involves peer-to-peer lending platforms, online lending marketplaces, and other digital solutions that connect borrowers and lenders with ease.

Total addressable market by 2030: USD 1.3 trillion

Neobanking

Digital-only financial institutions that leverage technology to provide a range of banking services, typically without the infrastructure associated with traditional banks.

Total addressable market by 2030: USD 74 billion

InsurTech

Leverages AI/ML and data analytics to modernise traditional insurance processes, enhance operational efficiency, provide more personalised insurance products, and create innovative solutions for risk assessment, underwriting, policy management, and claims processing.

Total addressable market by 2030: USD 307 billion

InvestmentTech

Transforms and optimises diverse aspects of investment and wealth management processes to provide individuals and institutions with improved investment strategies, portfolio management and financial advisory services.

Total addressable market by 2030: USD 31 billion

Payments

Fosters financial inclusion by providing convenient and accessible means for even the unbanked population to participate in economic transactions. This includes digital wallets, mobile payment apps, contactless payment solutions, and other electronic payment methods that improve the speed, security and accessibility of financial transactions.

Total addressable market by 2030: USD 53 billion

FinTech software as a service (SaaS)

Optimises operational efficiencies for financial institutions, specifically focusing on offering financial technology services, applications or platforms through a cloud-based subscription model.

Total addressable market by 2030: USD 18.3 billion

Source: Inc42, State of Indian FinTech report Q4 2023

03

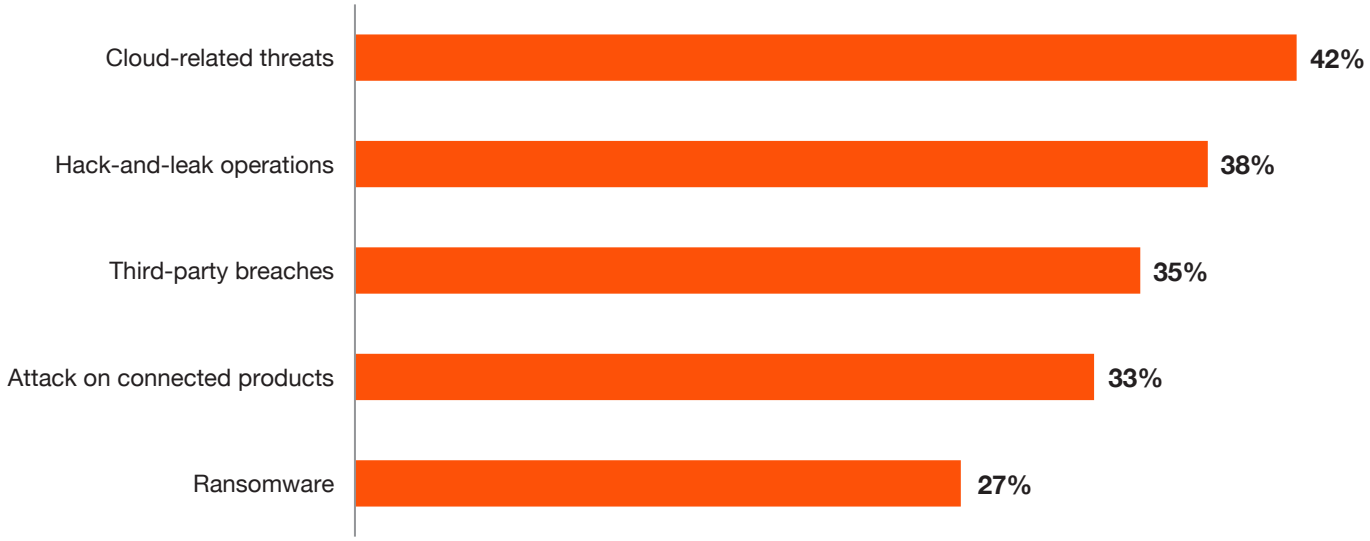
The FinTech firewall – current and emerging challenges

The junction of finance and technology presents a fertile ground for cyberthreats, as the digitalisation of financial services opens new avenues for malicious actors to exploit existing vulnerabilities. Cyberattacks are constantly targeting financial institutions. Data breaches and ransomware attacks have become increasingly sophisticated and frequent, posing a substantial risk to the solidity and integrity of the financial system.

3.1

CXOs' response to the current cyberthreat landscape

Our 2025 Global Digital Trust Insights report surveyed 4,042 business and technology executives from various organisations across the world. The most concerning cyber threats found in the sample could significantly affect how a business performs:



Source: PwC, 2025 Global Digital Trust Insights

What worries organisations most is what they're least prepared for.

According to our survey respondents, the top five cyberthreats are cloud-related threats (42%), hack-and-leak operations (38%), third-party breaches (35%), attacks on connected products (33%) and ransomware (27%). These are the same threats that security executives feel least prepared to address. This gap highlights the immediate need for more investments and better response capabilities.[14]

14 PwC, 2025 Global Digital Trust Insights

3.2

Current cybersecurity threats for FinTechs

1. Cloud-related threats

Given the current shift towards cloud services and infrastructure, cloud-related threats in FinTech are becoming more prevalent. Threat actors are exploiting cloud vulnerabilities, insecure APIs, misconfigured cloud settings and insufficient access and network security controls.

2. Ransomware attacks

Ransomware attacks continue to be major challenge for FinTech platforms, as they are lucrative targets for ransomware gangs due to the high-value data and urgency to restore operations.

3. Phishing and social engineering attacks

Cybercriminals and hackers have increasingly used targeted phishing emails and messages to steal login credentials for customers as well as employees.

Advanced fraud tactics like vishing (voice phishing) and deepfake scams make these attacks more convincing. Attackers attempt to impersonate as leaders or other authority figures to bypass security measures.

4. Supply chain attacks and third-party breaches

FinTech companies are heavily relying on third-party services such as cloud providers, analytics tools or any payment processors for daily business operations. However, these service providers often fail to maintain a robust cybersecurity posture. If a third party is compromised, attackers can exploit vulnerabilities to gain indirect access to the FinTech ecosystem which poses significant security risks.

5. API exploits

FinTechs heavily rely on APIs to enable integrations (e.g. with banks, payment gateways etc.). Insufficient security controls or poorly monitored APIs become the backdoor for attackers to access sensitive data or take control of critical systems.

6. Insider threats

Disgruntled employees or inadequately managed access controls can result in intentional or unintentional data leaks. Insiders have legitimate access to key systems and infrastructure, making their detection by security systems difficult. Also, the lack of privileged access management (PAM), behaviour monitoring capabilities and stringent access mechanisms results in elevated insider threats.

3.3

Emerging cybersecurity threats for FinTechs

Although emerging technologies in the FinTech space are catalysing innovation and growth, they are also giving rise to new cybersecurity threats and challenges. These cyber threats are constantly becoming more sophisticated and difficult to discover. Some of these threats for FinTechs have been highlighted below:

1. AI-enabled phishing attacks

Threats actors are leveraging AI to automate phishing and create personalised social engineering, bypassing anomaly detection. Such advanced AI-driven attacks can avoid traditional security controls and threaten the fraud detection and AML systems in FinTechs, thereby increasing the risk of data breaches and financial loss.

2. Deepfake and synthetic identity fraud

The increased use of deepfake videos, audio and documents is enabling the impersonation of individuals or executives during onboarding processes or significant approvals. This is jeopardising the know your customer (KYC) and anti-money laundering (AML) protocols, ignoring biometric verifications, and putting FinTech companies at risk of regulatory breaches and significant financial losses.

3. Quantum computing threats

The rapid integration and adoption of quantum technology is increasingly threatening the existence of current encryption standards like RSA, AES and ECC. Attackers can steal encrypted data and decrypt it later once quantum power becomes more mature, leading to 'harvest now, decrypt later' attacks that jeopardise long-term data confidentiality.

4. Compromised AI and algorithmic manipulation

FinTechs are increasingly using AI models across multiple areas such as credit scoring, lending and fraud detection. They face a significant threat from data poisoning or model inversion, which can lead to biased or erroneous decisions and reduce the overall model efficiency and accuracy.

5. Embedded finance and open banking API exploits

With the expansion of embedded finance, FinTech APIs are getting exposed to a broader ecosystem. Ineffective access controls are resulting in heightened risk of data fraud and unauthorised access, jeopardising the privacy of the customers and trust within interconnected financial services.

6. Cloud-native threats

Cloud migration inducts new risks such as container escapes, improperly configured storage and compromised cloud credentials. Cybercriminals take undue advantage of these vulnerabilities to access sensitive FinTech information or move laterally within the environment. This broadens the scope of the data breach and causes operational disruptions.

7. 5G and IoT payment infrastructure vulnerabilities

The onset of 5G technology and increased mobile payment option, such as wearables and smart POS, is resulting in increased cyberattacks due to emerging attack surfaces. Deficiencies in these systems can lead to botnet infiltration or man-in-the-middle attack which can hamper transaction security and pose privacy risks for user data.

8. DeFi and smart contract vulnerabilities

Decentralised finance (DeFi) platforms are dependent on smart contracts that are prone to coding flaws, oracle manipulation and rug pulls. Exploitation of these vulnerabilities can cause direct and irreversible financial losses without clear legal remedies. This also threatens the integrity and reliability of blockchain-integrated FinTech services.

9. Synthetic transaction fraud via automation tools

Bots and AI are making it easier to mimic true user behaviour to generate synthetic transactions which can help in bypassing fraud detection. This makes it more difficult to identify fraud and compromises FinTechs' fraud management mechanisms, leading to high financial risks.

3.4

Challenges faced by FinTechs in addressing cybersecurity needs

1. Rapid innovation outpacing security

FinTechs often prioritise rapid product releases over secure development, resulting in overlooked vulnerabilities. Security is frequently not integrated into DevSecOps pipelines which increases risk. This imbalance between speed and safety often exposes critical systems and infrastructure to cyber threats in an increasingly aggressive digital threat landscape.

2. Scalability of security infrastructure

As FinTechs scale, their security infrastructure must also expand accordingly and become more adaptable to handle heightened traffic, data volume and complexity without affecting the overall performance.

Scaling the infrastructure with the right set of tools and technologies poses technical and financial challenges.

3. Decreasing FinTech investments

Funding received by the FinTech sector has shown a declining trend which poses questions on overall growth of FinTech market in India and across the globe. In 2023, FinTech investments reached a five-year low of USD 39.22 billion globally as investors became cautious due to geopolitical and macroeconomic factor across the globe. The decreasing investment is also resulting in decreased spending across all the business functions including cybersecurity.[15]

4. Third-party risk management

FinTechs depend heavily on third-party providers, including cloud service providers and SaaS platform providers. These vendors may not consistently uphold security best practices which results in exploitation of theses vulnerabilities and deficiencies by threat actors.

5. Compliance with the evolving regulatory landscape

Adhering to the ever-evolving regulations from RBI, UIDAI, IDAI, Cert-In and DPDPA is difficult and poses compliance challenges for FinTechs. Continuous compliance management is resource-intensive, especially as businesses expand across multiple jurisdictions with varying standards and enforcement levels.

6. Hiring the right talent for specific security needs

Due to a constantly evolving threat environment, it is essential for FinTechs to maintain a competent workforce with adequate skills. The competition for qualified talent drives up costs, delays security initiatives and leaves organisations vulnerable.

15 PwC, FinTech – powering India's USD 5 trillion economy by fostering innovations, enabling inclusion and building a sustainable future

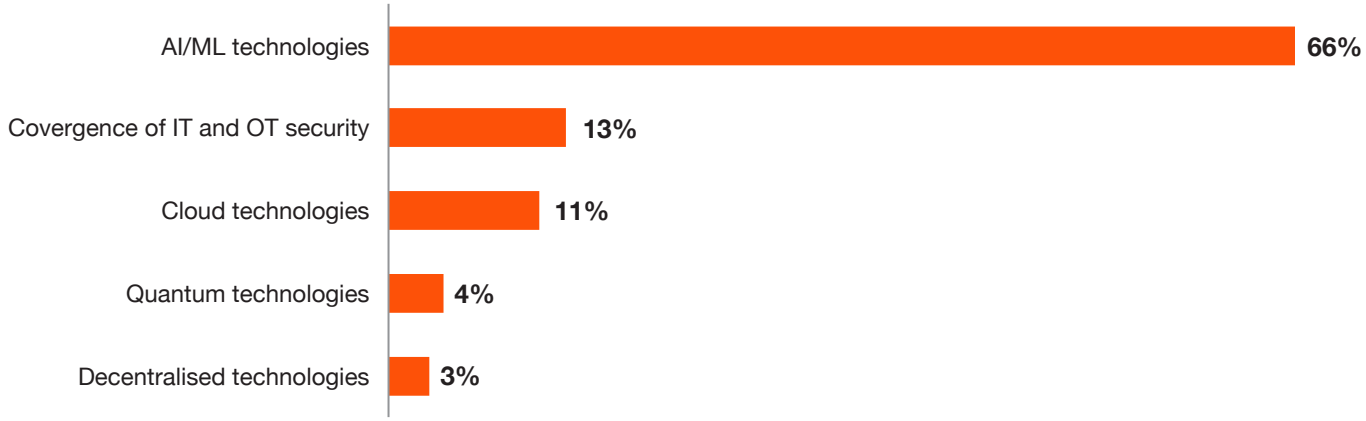
04

Technological advancements entailing cybersecurity

Rapid technological advancement is fuelling the growth of cybersecurity by creating new opportunities and posing new challenges. With digital systems becoming more complex and interconnected, vulnerabilities are also increasing, which is driving the demand for advanced cybersecurity measures. Innovations like AI, cloud computing and IoT require robust security solutions to protect data and privacy.

It is projected that few technologies would have a more significant impact in shaping the future of cybersecurity.

Most significant technologies to affect cybersecurity



Source: WEF Global Cyber Outlook 2025 report

According to the WEF GCO Survey 2025, 66% of organisations anticipate that AI will have the most significant impact on cybersecurity in the coming year. This is followed by the convergence of IT and OT security (13%), increased adoption of cloud technologies (11%), quantum technologies such as computing and encryption (4%), and decentralised technologies including secure multi-party computation and blockchain (3%).[16]

16 https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

05

Securing the future of FinTech – The security playbook

With the growing frequency and sophistication of cyberattacks targeting FinTech companies, it is imperative that these organisations reassess and strengthen their cybersecurity posture and strategies.

FinTechs can no longer solely rely on the traditional security models – they need to proactively rethink and revise their investments and frameworks to combat emerging threat vectors. The following aspects can be integrated into their existing defence mechanisms to enhance cyber resilience:

1. Cloud-native security

Adopting cloud-native security services and tools from cloud providers to improve security parameters. Enable real-time cloud visibility with investments in cloud native application protection technologies (open source is another option). Adopt cloud infrastructure management platforms, cloud security assessment software and solutions with a strategic approach.

2. Adopt zero trust architecture (ZTA)

FinTechs can implement a zero trust model where no user or system is trusted by default – all access requests (internal or external) are continuously authenticated, authorised and encrypted. Furthermore, micro-segmentation and real-time monitoring can help in significantly reducing breach risks and improving access control.

3. API security and secure DevOps

Integrate security mechanisms in the DevOps process so that security practices are deployed from the earliest stages of development. Additionally, implementation of API security mechanisms is also necessary. Protection of the entire lifetime of ongoing integrations and continuous deployment (CI/CD) pipeline is critical and includes static application security testing (SAST), dynamic application security testing (DAST), self-protection analysing programs and software configuration analysis solutions.

4. Leverage AI and ML for threat detection

Integrate AI and ML models to proactively detect threats and anomalies in real time. These systems can flag unusual transaction patterns or behaviour before an attack escalates, giving you a strong defence against fraud and cyberattacks – particularly in high-risk areas like KYC and payment systems.

5. Risk analysis of GenAI and large language models (LLMs)

Regularly perform comprehensive risk assessments for every GenAI platform/solution and LLM that is implemented, in addition to maintaining an up-to-date risk matrix. Conduct routine risk assessments to identify potential issues such as data contamination, model bias, synthetic identity fraud, deepfake amplification, emerging phishing techniques, privacy concerns, fairness concerns, information breaches and hallucinations.

6. Prepare with quantum-resistant cryptography

FinTechs may consider transitioning to quantum-resistant cryptography. With the evolution of quantum computing, current encryption methods would become vulnerable. Adopting post-quantum cryptographic standards that comply with NIST recommendations would guarantee the security of all systems and platforms against potential quantum threats in the future.

7. Deploy automated threat hunting tools

FinTechs shall deploy autonomous threat hunting systems that continuously scan for indicators of compromise (IOCs) to enhance their cybersecurity posture. These advanced threat hunting tools would help in reducing the overall dependence on manual detection, identify threats early, and minimise the chance of breaches or prolonged exposure.

8. Strengthen deepfake and synthetic fraud detection

As AI-generated media is becoming more mainstream, using real-time detection tools for deepfakes and synthetic identities is becoming more essential. Utilising these capabilities becomes more prevalent during customer onboarding and video KYC procedures. These tools would protect their platform from impersonation and social engineering attacks.

9. Integrate RegTech for real-time compliance

Implement RegTech solutions powered by AI and blockchain to automate compliance monitoring. This allows the organisations to stay ahead of evolving regulations without manual overhead. Real-time alerts and reporting ensure continuous compliance and audit readiness.

06

Regulatory developments in BFSI and its impact

Although India does not have a single, unified regulator for FinTech, the current BFSI sector regulators – such as the RBI, SEBI, IRDAI and UIDAI – are fostering a supportive environment for FinTech growth while ensuring necessary safeguards. Over the past year, FinTech companies are being empowered by regulators to take on a more significant role in payments, banking services, securities transactions and insurance. At the same time, regulators have prioritised enhancing customer protection and maintaining the stability of the financial system by imposing stronger governance and compliance requirements on FinTech firms.

According to the WEF's The Future of Global FinTech 2024 report, FinTech licencing, registration, inter-agency coordination and regulatory requirements remain among the most difficult challenges for FinTechs.[17]

Here are some of the recent regulations:

1	**RBI -** Master Directions on Cyber Resilience and Digital Payment Security Controls[18] **Circular:** RBI/DPSS/2024 25/123 (CO.DPSS. OVRST.no.S447/06 26 002/ 2024 25) **Issued:** 30 July 2024	• Strengthens cybersecurity mandates for payment system operators • Emphasises risk-based access, real-time fraud monitoring, incident reporting and system resilience for digital payments
2	**Digital Lending Framework –** RBI (Digital Lending) Directions, 2025[19] **Circular:** DOR.STR.REC.19/21.07.001/2025 26 **Issued:** 8 May 2025	• Revises and tightens norms for digital lending apps and platforms • Ensures transparency, data privacy, direct loan disbursal to borrower accounts and clear lender disclosures
3	**NPCI** - UPI API Usage Guidelines[20] **Circular:** NPCI/UPI/OC/215/2025 26 (with addendum OC/215A) **Issued:** 26 April and 21 May 2025	• Sets standards for UPI API call volumes, rate limits, failover protocols and app-level security • Mandates tighter API governance and audits for third-party application provider and payment service provider

17 WEF, The Future of Global FinTech 2024 report

18 https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=12715&Mode=0

19 https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12848&Mode=0

20 https://www.npci.org.in/PDF/npci/upi/circular/2025/UPI-OC-No-215-A-FY-2025-26-Guidelines-on-usage-of-UPI-APIs.pdf

4	**RBI -** Additional Factor Authentication – Card Transactions **Circular (Draft):** Draft AFA Framework for Digital Payments (July 2024)	• Proposes updates to additional factor authentication (AFA) for card-based digital transactions • Emphasis on context-aware AFA (e.g. risk-based or biometric triggers)
5	**IRDAI -** Cyber Incident and Crisis Preparedness Guideline[21] **Circular no.:** IRDAI/GA&HR/CIR/MISC/49/03/2025 **Date:** 24 March 2025	• Requires insurers to implement cyber incident response frameworks, regular crisis simulation exercises and threat intelligence sharing • Promotes a sector-wide coordinated response for digital insurance services
6	**MeitY -** Aadhaar Authentication for Good Governance Rules (SWIK–2025)[22] **Effective date:** 31 January 2025 Notification no. G.S.R. 88(E)	• Expands Aadhaar authentication for private and government entities for purposes such as welfare delivery, digital governance and FinTech inclusion • Introduces the SWIK portal for approval and onboarding

Non-adherence to these regulations by FinTech companies can lead to financial instability, data breaches and consumer distrust, which can cause an irreversible impact on the organisation. Furthermore, non-compliance may undermine legal safeguards, invite penalties and hamper industry credibility.

21 https://irdai.gov.in/document-detail?documentId=6975996

22 https://upload.indiacode.nic.in/showfile?actid=AC_CEN_37_85_00001_201618_1517807328460&type=rule&filename=swik_rules_-english_version.pdf

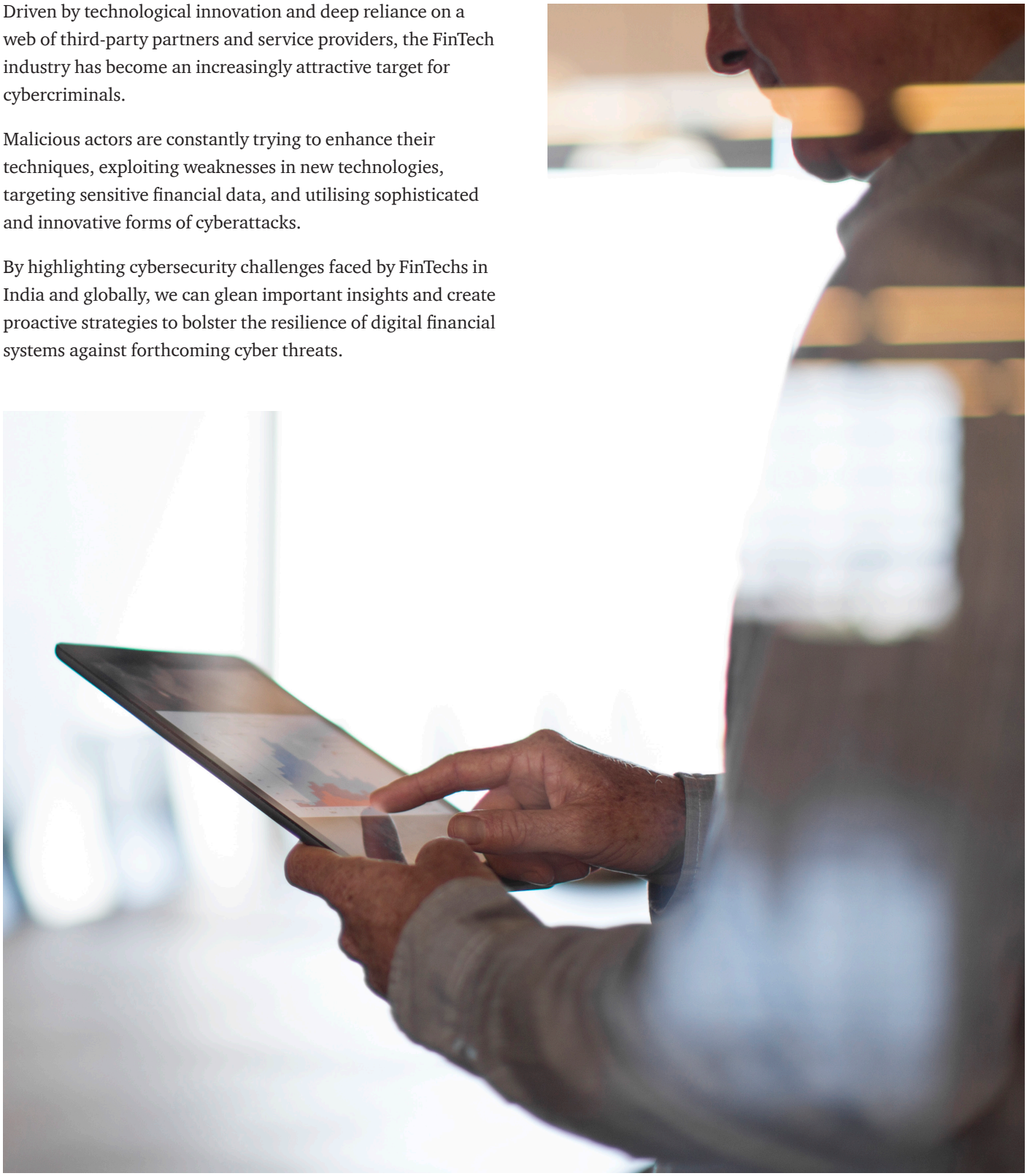
07

An overview of FinTech cyber breaches

Driven by technological innovation and deep reliance on a web of third-party partners and service providers, the FinTech industry has become an increasingly attractive target for cybercriminals.

Malicious actors are constantly trying to enhance their techniques, exploiting weaknesses in new technologies, targeting sensitive financial data, and utilising sophisticated and innovative forms of cyberattacks.

By highlighting cybersecurity challenges faced by FinTechs in India and globally, we can glean important insights and create proactive strategies to bolster the resilience of digital financial systems against forthcoming cyber threats.



Global	India
In mid-2017, a credit reporting agency's failure to apply software patches resulted in the exposure of personally identifiable information (SSNs, birthdates) of about 143 million US consumers, making it one of the most severe identity data breaches in history.[23]	In August 2020, a payments processing start-up in India experienced a data breach that exposed the card details of approximately 35 million users. The breach was a result of an unsecured server.[24]
A Japanese cryptocurrency exchange fell victim to a massive heist where hackers stole approximately USD 500 million worth of crypto coins in February 2018. The breach raised concerns about the security of cryptocurrency exchanges worldwide.[25]	In late 2020, a major payments solution provider discovered that around 35 million masked card entries and metadata (emails, phones) were accessed due to an unrecycled access key. The company only confirmed the details after dark web researchers exposed the data.[26]
In March 2022, a Canadian blockchain project lost USD 615 million in Ethereum and USD coin tokens in the second-largest cryptocurrency heist till date. In January 2024, a cross-chain cryptocurrency platform was hacked and experienced a wipe-off of USD 81 million from its trade balances.[27]	In April 2022, an Indian FinTech moneylending platform suffered a data breach where sensitive customer data containing more than 6.5 million files, totalling over 1 TB, was leaked online.[28]
In March 2023, an Australian financial services company faced a cyberattack wherein hackers stole ~14 million customer records –including driver's licences (7.9 million), passport numbers, financial statements etc. – by compromising a third-party vendor. The breach cost nearly AUD 95–105 million.[29]	In October 2023, a government API system experienced India's largest data breach where data of 81.5 crore Indian citizens was leaked.[30]
In January 2024, a global FinTech firm's operations were disrupted after some of its systems were taken offline through hacking.[31]	In June 2025, a group of hackers breached mobile application of a major financial services company in India, and stole nearly INR 1.95 crore worth of digital gold from the accounts of 435 customers.[32]

23 https://www.cnbc.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html
24 https://www.businesstoday.in/technology/news/story/amazon-swiggy-payments-partner-juspay-suffers-data-breach-35-crore-records-compromised-283598-2021-01-05
25 https://guardian.ng/news/japans-crypto-exchange-coincheck-sued-after-massive-heist/
26 https://www.businesstoday.in/technology/news/story/amazon-swiggy-payments-partner-juspay-suffers-data-breach-35-crore-records-compromised-283598-2021-01-05
27 https://www.reuters.com/technology/blockchain-company-ronin-hit-by-615-million-crypto-heist-2022-03-29/
28 https://www.the420.in/1-tb-data-leaked-online-personal-sensitive-information-of-customers-of-defunct-quick-loan-apps-breached/
29 https://www.theguardian.com/australia-news/2023/mar/27/latitude-financial-cyber-data-breach-hack-14m-customer-records-stolen
30 https://www.livemint.com/news/india/aadhaar-data-leak-massive-data-breach-exposes-815-million-indians-personal-information-on-dark-web-details-here-11698712793223.html
31 https://www.bleepingcomputer.com/news/security/global-FinTech-firm-equilend-offline-after-recent-cyberattack/
32 https://economictimes.indiatimes.com/industry/banking/finance/banking/aditya-birla-capital-app-hacked-digital-gold-worth-1-95-cr-stolen/articleshow/122104120.cms?from=mdr

08

Conclusion

India sits on a massive credit gap which is yet to be completely tapped. The attempt to fill this credit gap is being led by banks and NBFCs, followed by FinTechs – who are offering innovative products and cutting-edge solutions.

FinTechs have shown unprecedented growth in the past, and this momentum isn't slowing down anytime soon. But in order to sustain this growth, it's important to implement robust measures to fall back on – this is where cybersecurity plays a key role. Strengthening cybersecurity not only works as a defence mechanism, but also as a facilitator of a secure environment for growth.

As threats evolve, so must FinTechs. FinTech companies should constantly adopt next-gen cybersecurity tools and strategies that protect their innovation and secure their ecosystem.

Organisations are increasingly looking at cybersecurity as a key differentiator for achieving a competitive edge in the market. As cyber threats intensify, a strong and robust cybersecurity posture will enhance protection and help build a reputation that customers and stakeholders can rely on. At a time when trust is paramount, companies that prioritise cybersecurity are better positioned to stand out as leaders in both security and integrity.

Security isn't limited to setting up firewalls and encryptions anymore. A comprehensive outlook towards security now includes establishing and building trust among people, pertaining to the systems and processes involved.

About Unified Fintech Forum (UFF)

The Unified Fintech Forum (UFF), formerly known as the Digital Lenders Association of India (DLAI), stands as a pivotal non-profit Fintech sector Industry Association at the forefront of India's dynamic financial technology landscape. Established in October 2016 as a Section 8 company (not-for-profit) registered with the Ministry of Corporate Affairs, UFF has evolved significantly to represent the broader FinTech ecosystem. This mission and vision of UFF reflects the organization's commitment to fostering collaboration, innovation, and responsible growth across diverse FinTech domains, including payments, wealth tech, InsurTech and embedded finance.

UFF serves as a unified voice for myriad FinTech companies operating in India, playing a crucial role in shaping the regulatory environment, promoting best practices, and driving financial inclusion nationwide. Its current diverse membership base, exceeding 120 entities, encompasses regulated lenders (NBFCs, Banks), FinTech platforms, embedded finance players, technology providers, credit bureaus, legal firms, and industry advisors. This wide representation allows UFF to address the evolving needs of the sector comprehensively.

A core pillar of UFF's mission is client protection. Recognizing the accelerated adoption of FinTech services, UFF has proactively championed initiatives to safeguard consumer rights and interests, particularly for those accessing digital credit and other digital financial services. It was among the first industry bodies to introduce a Voluntary Code of Conduct for digital lenders, outlining clear principles on transparency, responsible lending, fair collection practices, grievance redressal, and data privacy. This code has served as a benchmark for ethical practices and has significantly informed regulatory policy, including the Reserve Bank of India's (RBI) digital lending guidelines. UFF also actively collaborates with consumer rights organizations and legal experts to address emerging risks like predatory lending and digital fraud, reinforcing trust and accountability in the FinTech space.

Beyond advocacy and client protection, UFF is deeply engaged in capacity building within the Indian FinTech ecosystem. It recognizes the rapidly evolving regulatory, technological, and business landscape and strives to equip stakeholders with the necessary knowledge and skills. UFF regularly conducts workshops, masterclasses, and webinars on critical topics such as regulatory compliance, data privacy, fraud prevention, and inclusive product design. These initiatives are tailored for FinTech founders, compliance professionals, product managers, and technologists. By developing toolkits, explainer notes, and checklists in collaboration with policy experts and regulators, UFF simplifies complex regulatory frameworks and operationalizes compliance, fostering a culture of continuous learning and responsible growth. UFF is committed to advancing best practices, maintaining regulatory adherence, and supporting innovation to further financial inclusion in India. The forum's work is instrumental in ensuring that India's FinTech revolution remains inclusive, sustainable, and globally influential.

Contact us

Jatinder Handoo
CEO
UFF
jatinhandoo@unifiedfintech.in

About PwC

We help you build trust so you can boldly reinvent

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 370,000 people in 149 countries. Across assurance, tax and legal, deals and consulting we help build, accelerate and sustain momentum. Find out more at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2025 PwC. All rights reserved.

Contact us

Sundareshwar Krishnamurthy
Partner, India Cyber leader
PwC India
sundareshwar.krishnamurthy@pwc.com

Amol Bhat
Partner – Risk Consulting and
Cybersecurity (Financial Services)
PwC India
amol.bhat@pwc.com

Shah Amber
Executive Director – Risk Consulting and
Cybersecurity (Financial Services - FinTech)
PwC India
shah.amber@pwc.com

Contributors

Mukul Kumar
Lisa Krishania
Pulkit Adlakha

pwc.in

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2025 PricewaterhouseCoopers Private Limited. All rights reserved.

HS/August 2025 - M&C 47765