



# Beyond the cloud: Navigating FinTech cyber threats and fortifying defences



## Unleashing innovation: An overview of India's FinTech landscape

In the midst of a rapidly evolving economy, India's FinTech sector has risen to exceptional heights – a result of revolutionary transformations driven by a combination of a disruptive environment, entrepreneurial spirit and technological competence. Digital revolutions arising from the intersection of technology and finance have not only redefined existing paradigms but are also driving the entire Indian financial industry to new frontiers of possibilities.

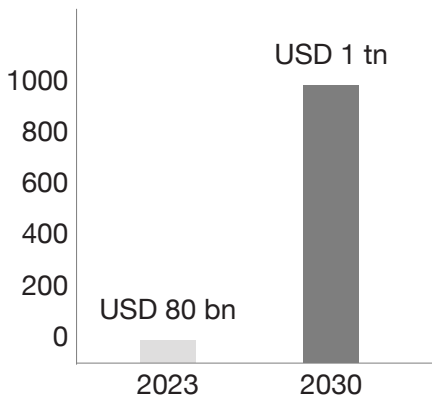
Over the last decade, the Indian FinTech industry has undergone an accelerated metamorphosis. Peer-to-peer lending platforms, digital wallets, mobile payment systems and robo advisors have fundamentally changed the way people conduct financial transactions. Government programmes that supported the push for a cashless economy and introduced the Unified Payments Interface (UPI) – which as of March 2024 witnessed record transaction values of USD 237.5 billion<sup>1</sup> – have further sped up this transition. As of early 2024, the number of smartphone users in India stands at 1.12 billion<sup>2</sup> and is rising. This can be attributed to the year-on-year growth in the number of mobile connections, with the first quarter of 2024 recording 23 million<sup>3</sup> (+2.1%) more mobile connections in India than the start of 2023. Alongside smartphones, India's internet user base has also soared to 751.5 million<sup>4</sup> at the start of 2024. These figures indicate a solid foundation for incentivising and driving cutting-edge FinTech innovations that upscale financial accessibility and digital inclusion.



# FinTech market horizon: A quick overview of key FinTech sectors

Millions of underbanked and unbanked individuals today have democratised access to financial services due to the pivotal role played by FinTechs. The FinTech industry in India is currently undergoing significant expansion. In 2023, the FinTech industry market went beyond the USD 80 billion mark and is expected to grow into a USD 1 trillion market by 2030.<sup>5</sup> Q 1 of 2024 saw total FinTech sector funding rise to USD 551 million, up by 59% as compared to Q3 of 2023(USD 346 million).<sup>6</sup>

## Indian FinTech market size



Source: <https://www.businesstoday.in/opinion/columns/story/fintech-trends-2024-a-retrospective-deep-dive-428636-2024-05-07>

The Indian fintech market is essentially divided into multiple sub-sectors, each catering to very specific and unique aspects of financial services. Fundamentally, there are six main sub-sectors that collectively make up the fintech sector. A short examination of these fintech market segments reveal the many multifaceted ways in which technological advancements are influencing and enhancing several aspects of the financial sector.

1. <https://www.npci.org.in/what-we-do/upi/product-statistics>  
2. <https://datareportal.com/reports/digital-2024-india>  
3. Ibid.  
4. Ibid.  
5. <https://www.businesstoday.in/opinion/columns/story/fintech-trends-2024-a-retrospective-deep-dive-428636-2024-05-07>  
6. <https://www.zeebiz.com/india/news-indias-fintech-sector-logs-robust-59-percent-growth-in-q1-2024-283938>

## Indian FinTech sub-sector market size: 2030 forecasts

<b>LendingTech</b>  Market size 2030: USD 1.3 tn	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.
<b>InsurTech</b>  Market size 2030: USD 307 bn	Leverages artificial intelligence (AI)/machine learning (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.
<b>Payments</b>  Market size 2030: USD 53 bn	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.
<b>Neobanking</b>  Market Size 2030: \$74 bn	Digital-only financial institutions that leverage technology to provide a range of banking services, typically without the infrastructure associated with traditional banks.
<b>InvestmentTech</b>  Market size 2030: USD 31 bn	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.
<b>FinTech software as a service (SaaS)</b>  Market size 2030: USD 18.3 bn	Optimises operational efficiencies for financial institutions, specifically focusing on offering financial technology services, applications or platforms through a cloud-based subscription model.

Source: State of Indian Fintech report Q4 2023, Inc42

tn = trillion

bn = billion

These sub-sectors have emerged as powerful disruptors, challenging traditional banking methodologies and undoing regressive operating silos.

While strong synergies led by government frameworks and FinTech innovations continue to transform the FinTech space, the upward trajectory of the industry is not without its challenges. The escalating risks posed by novel cybersecurity threats are the one of the most pressing concerns for FinTechs today.

Due to their continued endeavour to offer innovative financial solutions that capitalise on the cutting-edge capabilities of advanced technologies like blockchain, AI/ML and cloud computing, FinTechs have emerged as lucrative targets for cybercriminals intent on exploiting vulnerabilities within these sophisticated systems.

And thus, it is of critical importance for FinTechs to (1) understand where the risks are stemming from; (2) isolate them to minimise disruptions; and (3) implement robust cybersecurity measures to keep pace with the growing interconnectedness of digital financial services. Since FinTechs handle an immense volume of sensitive data, it becomes imperative for these platforms to focus on conscious strategic investments in cutting-edge cybersecurity solutions and maintain constant vigilance on the operations of their newly adopted advanced technologies.



## Cybersecurity in focus: Rise of global cyberthreats

As technology continues to evolve, FinTechs, whether domestic or global, face persistent headwinds from emerging cyberthreats, security failures and data breaches. The continuous impact of geopolitical instabilities, rapid advancement of digitisation and escalating sophistication of cybercriminal tactics pose a threat to the industry's remarkable growth trajectory.

Within just a decade, global companies are estimated to incur a surge in annual cybercrime expenses, approximately up to USD 10.5 trillion – a significant increase from the USD 3 trillion recorded in 2015.<sup>7</sup> The interconnectedness of global economies further amplifies the impact of cyber malpractices, with an incident in one region capable of triggering a domino effect across borders. The increasing frequency and severity of cyberattacks underscore the need for an intensified focus on cybersecurity.

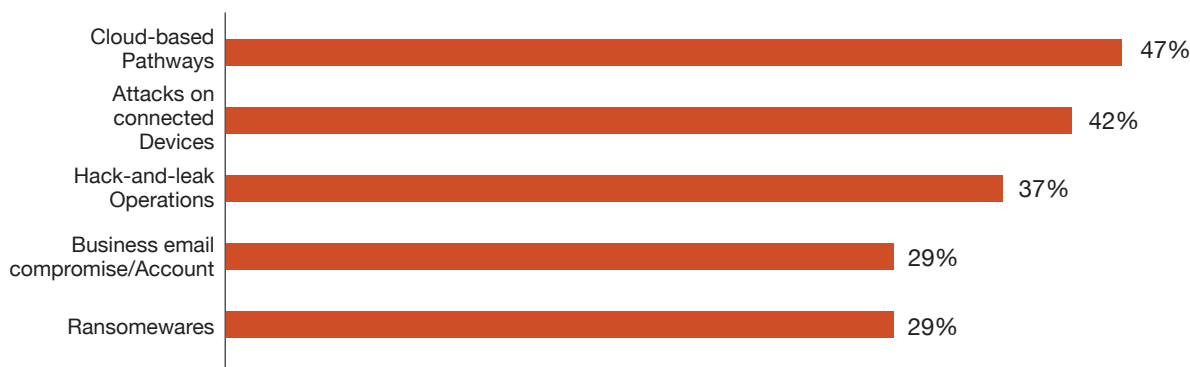
In light of these challenges, the modern cyber risk landscape demands a holistic approach, necessitating the deployment of advanced threat detection software, proactive risk mitigation mechanisms and resilient incident response strategies. This heightened cybersecurity focus is not solely reactive but anticipatory, as more and more FinTechs strive to stay one step ahead of the evolving threat landscape. As a result, their cybersecurity strategy has shifted to prioritising investments that will enhance the agility of response mechanisms, ultimately fostering a resilient cybersecurity culture.



## Top cybersecurity threats for global enterprises

As part of PwC's 2024 Global Digital Trust Insights survey,<sup>8</sup> approximately 4,000 CXOs ranked the most significant cybersecurity threats faced by their organisations. Notably, of eleven identified threats, the top three were cloud-based pathways, attacks on connected devices, and hack-and-leak operations. These findings underscore the evolving nature of cyberthreats, with an emphasis on the vulnerabilities associated with digital interconnectedness.

## How CXOs ranked threats that are relevant to their firm



Source: PwC's 2024 Global Digital Trust Insights

The ranking of business email compromises and account takeovers as the fourth top threat adds complexity to this landscape. Since cyberthreats do not occur in a standardised format across firms, a one-size-fits-all risk management solution cannot be the answer.

Only a tailored and carefully designed cybersecurity strategy that exclusively caters to the nature of the operating models of FinTechs will efficiently address the unique challenges posed by various vectors such as cloud vulnerabilities, interconnected devices/pathways, and the increasing sophistication of cyberthreats.

## Mapping the risk: A brief statistical overview of major cyberthreat types

As the digitisation landscape expands, so do the cyberattack vectors. While FinTechs are increasingly adopting cloud services, embracing IT modernisation and integrating traditional silos with cutting-edge AI/ML solutions, cyberattackers are also casting their netwide.

The Indian Computer Emergency Response Team (CERT-In)<sup>9</sup> reported 4,29,847 cybersecurity incidents pertaining to financial institutions in 2023, up from 6,168 in 2019. This highlights a sharp increase in cybercrime following the digital shift post the COVID-19 pandemic.

7. <https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/>

8. <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html>





## Ransomware attacks

Due to its integration of advanced digital payment systems along with other solutions for the banking sector that use complex AI/ML algorithms, the FinTech sector has grown more susceptible to ransomware attacks. Since FinTech companies manage vast volumes of sensitive financial data – transaction details, client records and payment information, among other things – cybercriminals profit greatly. Digital wallets and adoption of cloud computing expand the attack surface even further. FinTech networks are often infiltrated using methods such as spear-phishing, exploit kits and zero-day vulnerabilities. Furthermore, the spread of platforms for ransomware-as-a-service (RaaS) has lowered the entry barriers for criminals, raising the frequency and complexity of attacks.

There was a record 70% increase in global ransomware attacks in 2023 over the previous year.<sup>10</sup> While North America experienced maximum ransomware attacks (59%), Asia-Pacific suffered 12% of the attacks in Q1 2024. In terms of country-wise attack vectors, India emerged among the top targeted nations, with an organisation facing an average of 2,807 attacks per week in Q1 2024.<sup>11</sup>

According to the Data Security Council of India (DSCI),<sup>12</sup> for every 650 cyber malware incident it detects, a single ransomware security incident is reported. Between October 2022 to September 2023, 740,000 ransomware detections were reported within organisations. FakeUpdates, a botnet and downloader, remote access trojans and botnets were identified as the top malwares targeting Indian firms.<sup>13</sup>

FinTechs continuously evolve their technology use cases to offer more innovative solutions. Such accelerations in integrating and adopting advanced and emerging technologies have made FinTechs attractive target for ransomware attacks.

## Data breach costs

Owing to the enormous volumes of financial and personally identifiable information (PII) that FinTech businesses handle, the industry is particularly vulnerable to malicious breach incidents. FinTechs today play a major role in bridging the gap between the traditional silos of banking systems and digitalisation. In a quest for improving service delivery, FinTechs use technologies like application programming interfaces (APIs), mobile banking applications and real-time payment processing systems, which lowers the barriers against data breaches. Cybercriminals frequently exploit weak encryption methods, poor access restrictions and misconfigured cloud storage services to gain access to valuable data.

The World Economic Forum highlighted a sharp spike in global data breach numbers in 2023, with data compromises increasing by 72% over the previous year.<sup>14</sup>

---

8. <https://economictimes.indiatimes.com/tech/technology/over-1-lakh-cyber-security-incidents-in-govt-organisations-this-year/articleshow/102362589.cms?from=mdr>

9. <https://www.prnewswire.com/news-releases/q1-2024-sets-record-for-most-global-ransomware-attacks-in-a-first-quarter-new-corvus-insurance-ransomware-report-302131045.html>

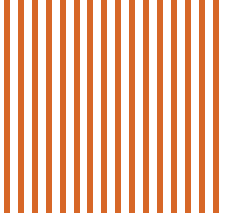
10. <https://www.prnewswire.com/news-releases/q1-2024-sets-record-for-most-global-ransomware-attacks-in-a-first-quarter-new-corvus-insurance-ransomware-report-302131045.html>

11. <https://timesofindia.indiatimes.com/technology/tech-news/cyber-attacks-surge-globally-in-q1-2024-india-among-most-targeted-nations-report/articleshow/110041081.cms>

12. <https://www.dsci.in/files/content/knowledge-centre/2024/India%20Cybersecurity%20Domestic%20Market%202023.pdf>

13. <https://timesofindia.indiatimes.com/technology/tech-news/cyber-attacks-surge-globally-in-q1-2024-india-among-most-targeted-nations-report/articleshow/110041081.cms>

14. <https://www.weforum.org/agenda/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/>



The DSCI stated that the global average cost of a data breach<sup>15</sup> was USD 4.45 million in 2023. From 2019 to mid-2023, India witnessed a total of 186 data breaches and 62 data leak incidents. The financial ramifications of these cyberthreats are thus a cause for concern among organisations across sectors.

According to the 2023 Data Breach Investigations report by Verizon,<sup>16</sup> of the nearly 10 lakh cybercrime incidents analysed worldwide, nearly 2.6 lakh were confirmed breaches. The incidents triggered financial losses ranging from USD 1 to USD 2.25 million, while the calculated average cost of a breach for a firm stood at USD 26,000. This large sum includes a variety of costs, such as legal fees, consumer notices, inquiries and reputation damage control.

## Insider threats

FinTechs today are experiencing immense growth with amplified CAGR figures backing their accelerated rise. However, as FinTechs often operate in fast-paced environments, innovating solutions swiftly to maintain their competitive edge in the market, they often fall short in terms of having appropriate control measures and oversight in place. FinTechs deal with highly sensitive data built into their payment gateways and APIs, where the highest levels of access are often granted to a limited number of employees. This encourages malicious actors to easily misuse their authority and capitalise on their deep subject-matter knowledge to exploit sensitive information. However, on the other hand, it becomes difficult to distinguish if such threats stem from unintentional human errors or oversights – i.e. genuine mistakes by employees or a lack of awareness about security protocols – thus rendering business pathways exposed and vulnerable.

According to the Verizon 2024 Data Breach Investigations Report,<sup>17</sup> more than 85% breaches were termed as insider threats that were reported within the category of human element-related incidents. The main driving motives behind such breaches were mainly financial (88%), closely followed by company secrets revelation (46%). Malicious insiders mostly targeted personal data of employees, clients and contractors (83%), while internal data (sensitive plans, strategies and intellectual property – 46%) was reported stolen for illegal data sale to external sources.

In terms of unintentional errors caused by employees, personal data was highlighted as the most compromised data (94%), while internal business-sensitive data – which also included top management and client personal data – was erroneously compromised as well (34%), leading to larger subset of unintended insider threats.

FinTechs, in order to plug cyber risks, must therefore consider both unintentional and malicious insider threats and re-evaluate their data protection controls and security infrastructure and conduct insider awareness training programmes for employees periodically.

---

15. <https://www.dsci.in/files/content/knowledge-centre/2024/India%20Cybersecurity%20Domestic%20Market%202023.pdf>

16. <https://www.verizon.com/business/resources/reports/dbir/2023/master-guide/>

17. <https://www.verizon.com/business/resources/Tb06/reports/2024-dbir-data-breach-investigations-report.pdf>





## Supply chain and third-party threats

For critical functions such as payment gateways, cloud hosting and cybersecurity solutions, FinTechs often depend on an intricate network of third-party vendors and service providers. However, overreliance on third parties tends to introduce significant supply chain risks, as any weaknesses existing in third-party networks may jeopardise the security of the entire FinTech ecosystem. For instance, hacking of an API provider or third-party payment processor might expose a large quantum of data and trigger operational interruptions. These risks are further heightened by the absence of continuous monitoring of third-party security practices, insufficient vendor verification processes and inadequate contractual safeguards. In an effort to indirectly infiltrate FinTech networks, cybercriminals are increasingly employing sophisticated supply chain attack techniques, which involve the introduction of malware directly into software updates and/or development tools.

Furthermore, in today's software-driven environment, cybercriminals are constantly on the lookout to compromise multiple supply chains simultaneously. By 2025, more than 45% of organisations will suffer from compromises within supply chains.<sup>18</sup> Moreover, attacks on software supply chains take up a prominent share in India, accounting for about 59.4%<sup>19</sup> of the total cybersecurity attacks in the country.

According to a survey on Global Cybersecurity Outlook 2024<sup>20</sup> by the World Economic Forum, 41% of organisations reported a material incident that originated from a third-party collaborator in 2023.

PwC India's Global Digital Trust Insights Report 2024<sup>21</sup> emphasised that 35% of Indian organisations identify coping with software supply chain compromises as their primary cyberthreat in the next 12 months.

### Cybersecurity lens: Discussing cybersecurity incidents within global and Indian FinTechs

The FinTech sector, characterised by its innovative use of technology and interconnected nature which includes numerous third-party vendors and partners, has increasingly become a lucrative target to malicious attacks by cybercriminals.

As the industry experiences rapid growth in digitisation, vulnerabilities emerge as a common denominator. Cyber adversaries continuously update their tactics, exploiting vulnerabilities in emerging technologies, targeting sensitive financial data, and deploying novel and sophisticated cyber malpractice schemes. In addition to compromising sensitive financial information of millions of users, these vulnerabilities also breach users' trust in digital financial services.

Based on noteworthy cases and emerging trends, our objective is to highlight the diverse challenges encountered by FinTech companies. By gaining insights from each incident, we aim to derive valuable lessons that can help take proactive measures in order to fortify digital financial ecosystems against potential cyberthreats.

---

18. <https://www.forbes.com/sites/forbestechcouncil/2024/02/06/rising-threat-understanding-software-supply-chain-cyberattacks-and-protecting-against-them/>

19. <https://www.dsai.in/files/content/knowledge-centre/2024/India%20Cybersecurity%20Domestic%20Market%202023.pdf>

20. [https://www3.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2024.pdf](https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf)

21. <https://www.pwc.in/assets/pdfs/digital-trust-insights-india/digital-trust-insights-india.pdf>

## FinTech cyberthreat incidents

Global	India
1 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. <sup>22</sup>	In April 2018, an Indian cryptocurrency exchange reported a security breach. The exchange's hot wallet was compromised, resulting in the theft of 438 Bitcoin (BTC) <sup>23</sup> worth millions of dollars.
2 In 2019, a popular stock and cryptocurrency trading platform was targeted malicious entities, who gained unauthorised access and stole email addresses of customers. The incident affected more than 5 million users. <sup>24</sup>	In August 2020, a payment processing start-up in India experienced a data breach that exposed the card details of approximately 35 million users. <sup>25</sup> The breach was a result of an unsecured server.
3 In March 2022, a Canadian blockchain project lost USD 615 million <sup>26</sup> in ether and USD coin tokens in the second-largest cryptocurrency heist to date.	In April 2022, an Indian FinTech moneylending platform <sup>27</sup> suffered a data breach where sensitive customer data containing more than 6.5 million files, totalling over 1TB, was leaked online.
4 In January 2024, a cross-chain cryptocurrency platform was hacked and experienced a wipe-off of USD 81 million <sup>28</sup> from its trade balances.	In August 2022, a digital financial services <sup>29</sup> provider in India experienced a major data breach resulting in the exposure of personal data and transaction details of approximately 37,000 users.
5 In January 2024, a global FinTech <sup>30</sup> firm's operations were disrupted after some of its systems were taken offline through hacking.	In October 2023, a Government API system experienced India's largest data breach where 81.5 crore <sup>31</sup> Indians' data was leaked.

22. <https://guardian.ng/news/japans-crypto-exchange-coincheck-sued-after-massive-heist/>

23. <https://www.businesstoday.in/latest/economy-politics/story/bitcoin-theft-coinsecure-hack-bitcoins-exchange-india-19-crore-104978-2018-04-13>

24. <https://www.cnbc.com/2021/11/09/robinhood-data-breach-involved-7-million-clients-protect-your-credit.html>

25. <https://www.businesstoday.in/technology/news/story/amazon-swiggy-payments-partner-juspay-suffers-data-breach-35-crore-records-compromised-283598-2021-01-05>

26. <https://www.reuters.com/technology/blockchain-company-ronin-hit-by-615-million-crypto-heist-2022-03-29/>

27. <https://www.the420.in/1-tb-data-leaked-online-personal-sensitive-information-of-customers-of-defunct-quick-loan-apps-breached/>

Key threats to look out for in cloud-enabled FinTechs



FinTechs must recognise the evolving landscape of sophisticated cloud-enabled cybersecurity threats. Moreover, the interconnected nature of cloud environments heightens the risk of data security compromises, where attackers exploit numerous weaknesses.

28. <https://cryptodaily.co.uk/2024/01/hackers-ring-in-new-year-with-massive-81m-orbit-chain-exploit>

29. <https://ciso.economictimes.indiatimes.com/news/bharatpay-finance-services-breached-personal-data-transaction-details-of-37000-users-leaked-online/93586873>

30. <https://www.bleepingcomputer.com/news/security/global-fintech-firm-equilend-offline-after-recent-cyberattack/>

31. <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>



## PwC's cybersecurity recommendations to support FinTech growth

Considering the increasing number of cyberattacks on FinTechs, companies must shift their focus towards re-strategising their current cybersecurity investments and frameworks in order to prevent/halt the dire implications of evolving cyberthreat vectors. To do so, FinTechs can include the following recommendations within their existing cyber defence mechanisms and frameworks:

**1.Cloud-native security:** Adopt 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.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 application programming interface (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.

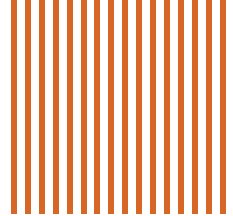
**3.Identity and access management (IDAM):** To ensure access or entry points are solely restricted to authorised personnel only, implement IDAM solutions to supervise and regulate access to resources. Monitor overprovisioned access/privileges and shadow accesses. Multi-factor authorisation (MFA) should be mandatorily deployed for contractors/vendors and should be considered for every employee/staff.

**4.Implementation of ML and AI solutions:** To predict and potentially protect against emerging cyber risks, adopt advanced AI/ML-powered models and algorithms. Detailed language models, predictive intelligence, and behaviour analytics solutions are designed to detect anomalies by identifying patterns in large data sets. Potential threats can be detected on a real-time basis with the help of such system deployments.

**5.Continuous monitoring and audit, security testing and compliance:** Ensure the security of your cloud infrastructure and applications via periodic security assessments, penetration testing, security audits, etc. Stay up to date on financial industry regulations such as General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS) and Digital Personal Data Protection (DPDP) for robust compliance with financial industry regulations.

**6.Incident response plan:** Develop and periodically test an incident response plan outlining a step-by-step list of activities to be carried out in the event of a security breach. Real-time responses are generated by adaptive security decision-making processes so as to maintain an advantage over cybercriminals' strategies.

**7.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, evolving phishing techniques, privacy concerns, information breaches, fairness concerns and hallucinations.



**8.Training and awareness for employees:** Promote a culture that prioritises security by conducting regular cybersecurity training programmes for all employees. This should cover common vulnerabilities such as shadow IT, phishing, GenAI-based risks, deepfakes and any other related cyberattacks that may be triggered by user-level errors.

**9.Strengthen risk culture:** Promote a risk-conscious culture that prioritises security and is led from the top down. A firm's cybersecurity practices become deeply embedded into its culture when they are prioritised by senior management and incorporated into the agenda of the boardroom.

**10.Regulatory compliance:** Mandatorily adhere to existing regulatory frameworks and be up to date with newly introduced or upcoming regulations to ensure maximised data security and consumer protection. Compliance with the Reserve Bank of India (RBI)'s guidelines is crucial, including the Payment and Settlement Systems Act, 2007, Digital Lending Guidelines, 2022, and Digital Payment Security Controls, 2021. Furthermore, companies must implement measures to comply with RBI's mandates on data localisation and cybersecurity controls, and conduct periodic audits. For instance, adherence to regulations such as the Digital Personal Data Protection (DPDP) Act, 2023, ensures stringent protection of consumer data.

## The way forward

With a growing gig economy and increasing investor pressure to gain exponential returns, it is imperative that cloud-native technology companies, especially FinTechs, prioritise cybersecurity and embed the required controls into the design of their ecosystems. It is prudent for organisations to have maximum visibility into the world of pertinent threat actors that are constantly targeting the FinTech space and take proactive measures in terms of technology, collaboration, awareness, response and vision to mitigate any potential risks. Additionally, it is important to pay attention to individual/isolated events like data breaches, ransomware attacks, distributed denial-of-service (DDoS), privilege escalation, information manipulation and supply chain attacks, which can cause significant reputational, financial, regulatory and psychological damage both in the short and long term.

As threat vectors evolve along with the adoption and integration of modernised technology, it is crucial for firms to remain a step ahead of the cyber malpractice curve. The consistent rise of global cyberthreats underscores the need for an aggressive yet adaptive cybersecurity approach. This can be done by carefully examining the causal factors for these incidents and chalking out potential cyberattack pathways based on the firm's nature and scope of operations.

Once these cyber risks are intrinsically decoded, firms can proactively strategise cybersecurity investments and design holistic security measures to not only limit data exposures and counteract potential threats, but also fortify their digital defences against evolving threats arising from the integration of advanced technology.

# About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at [www.pwc.com](http://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](http://www.pwc.com/structure) for further details.

© 2024 PwC. All rights reserved.

## Contact us

### Siddharth Vishwanath

Partner and Risk Consulting Domestic Market Leader,  
PwC India  
[siddharth.vishwanath@pwc.com](mailto:siddharth.vishwanath@pwc.com)

### Sundareshwar Krishnamurthy

Partner – Risk Consulting and Leader Cybersecurity,  
PwC India  
[sundareshwar.krishnamurthy@pwc.com](mailto:sundareshwar.krishnamurthy@pwc.com)

### Manu Dwivedi

Partner – Risk Consulting and Leader Cybersecurity,  
Risk Consulting GCC, PwC India

### Dhruv Gupta

Director – Cyber Deals, PwC India  
[dhruv.d.gupta@pwc.com](mailto:dhruv.d.gupta@pwc.com)

## Contributors

Siddharth Vishwanath  
Dhruv Gupta  
Priyanjali Moulik

## Editorial

Dion D'Souza  
Rashi Gupta

## Design

Arvind Bachheti

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.

© 2024 PricewaterhouseCoopers Private Limited. All rights reserved.