

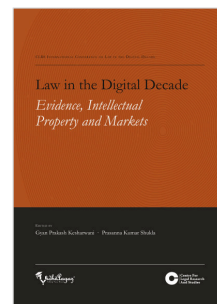
CHAPTER 18

Cyber Risk Insurance for Fintech and Digital Payments: Regulatory Challenges and Emerging Coverage Gaps in India

Sowmya. H.A

in *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla (VidhiAagaz 2026), pp. 191–206

DOI <https://doi.org/10.63108/VAB.LDD.2.18>



CITATIONS

BLUEBOOK (21ST ED.)

Sowmya. H.A, *Cyber Risk Insurance for Fintech and Digital Payments: Regulatory Challenges and Emerging Coverage Gaps in India*, in *LAW IN THE DIGITAL DECADE: EVIDENCE, INTELLECTUAL PROPERTY AND MARKETS* 191 (Gyan Prakash Kesharwani & Prasanna Kumar Shukla eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Sowmya. H.A, 'Cyber Risk Insurance for Fintech and Digital Payments: Regulatory Challenges and Emerging Coverage Gaps in India' in Gyan Prakash Kesharwani and Prasanna Kumar Shukla (eds), *Law in the Digital Decade: Evidence, Intellectual Property and Markets* (VidhiAagaz 2026) 191.

CHICAGO (17TH ED.)

Sowmya., H.A. "Cyber Risk Insurance for Fintech and Digital Payments: Regulatory Challenges and Emerging Coverage Gaps in India." In *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla, 191–206. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.2.18>.

APA (7TH ED.)

Sowmya., H. A. (2026). Cyber risk insurance for fintech and digital payments: Regulatory challenges and emerging coverage gaps in India. In G. P. Kesharwani & P. K. Shukla (Eds.), *Law in the digital decade: Evidence, intellectual property and markets* (pp. 191–206). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.2.18>

SOURCE

<https://doi.org/10.63108/VAB.LDD.2.18>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 18

Cyber Risk Insurance for Fintech and Digital Payments: Regulatory Challenges and Emerging Coverage Gaps in India

SOWMYA. H.A.*

Fintech platforms have shown an explosive growth with the rapid adoption of digital payments. However, the same has exposed especially Indian fintech and digital payment platforms to cyber risks, i.e., incidents such as phishing, payment fraud, ransomware, data breaches, identity theft, system disruption, etc. Moreover, companies and businesses have become more vulnerable to third-party incidents due to increased exposure to the cyber domain. Cyber risk insurance is one of the mechanisms to mitigate risks by transferring the financial losses to the insurer.

However, it is not clear whether the existing legal provisions and insurance policies provide sufficient coverage for fintech and digital payment platforms. This paper examines the question, to what extent does the existing legal framework facilitate cyber risk insurance, and how effective is it in managing the emerging cyber risks in India?

The paper adopts doctrinal and analytical approaches to study the relevant sections of the legislation, regulatory directives, and judicial developments. The paper also examines the regulatory frameworks of payment and cyber risks by the Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority of India (IRDAI) and addresses the growing concerns in fintech ecosystems.

International practices are also examined based on existing regulatory frameworks for cyber and digital payment risks and cyber risk insurance, and their relevance to India is identified.

The paper concludes that the regulatory framework in India for cyber risk and digital payments is evolving to identify gaps in risk transfer, thereby highlighting the need for a progressive approach in cyber risk insurance. The paper identifies relevant regulatory actions and reforms to address these emerging gaps.

Keywords: Cyber Risk Insurance, Cybersecurity Regulation, Data Breach, Digital Payments, Fintech.

1 INTRODUCTION

The financial industry in India is evolving rapidly, with a digital revolution in the delivery of banking, payment and other financial services. The emergence of banking services, electronic wallets, payment aggregators, mobile applications, internet banking, Unified Payments Interface (UPI), pre-paid instruments and other technology-driven financial services has led to the formation of an integrated financial ecosystem where most financial transactions can be completed in an almost instant manner. The new financial services have boosted financial inclusion and convenience but also pose new risks. The bigger the number of participants in a digital financial transaction, the greater the impact of a cyber incident. A

* PhD Scholar at KLE Law College (A Constituent College of KLE Technological University), Bengaluru, Karnataka, India.

disruption in a technology platform or service provider can have a knock-on impact on merchants, customers, financial institutions and other stakeholders in the payment ecosystem.¹

The rapid expansion of digital payments has altered the profile of financial risk. Whilst traditional financial risks such as credit risk, liquidity risk and market risk remain and continue to evolve, this is increasingly exacerbated by cyber risks that threaten the confidentiality, integrity and availability of digital financial infrastructure. A successful cyberattack could result in direct financial loss but also involve regulatory sanctions, litigation costs, reputational damage, business disruption and erosion of consumer confidence. Moreover, because digital financial transactions are performed via networked platforms, including banks, payment systems and fintechs and technology and other service providers, the damages could extend beyond the financial institutions directly affected.²

Accordingly, cyber risk insurance has become increasingly important as a vehicle for transferring certain of the financial consequences of cyber incidents. However, insurance cannot replace cyber control measures and is rather seen as a line of defence providing financial protection when an insured event occurs. Therefore, the relationship between cyber regulation and cyber insurance is a key point of consideration in the fintech environment. In this context, RBI has been significantly tightening its oversight of cyber risk at various levels of financial institutions and payment system participants, and IRDAI has been creating policy direction for cyber insurance products.³

Cyber risk insurance is a relatively new risk transfer mechanism for covering losses resulting from cyber events. The effectiveness of cyber risk insurance in the Indian context depends critically upon coordination between the insurance and cybersecurity regulatory regimes. Cybersecurity regulations form the basis for establishing the controls expected of an organisation, whereas insurance contracts form the basis for determining everything that constitutes coverage and the extent of indemnification. Disputes arising between insurers and insureds over the interpretation and application of policy exclusions and warranties, disclosure obligations, causation and the classification of losses are amongst the challenges faced in the application of cyber insurance.⁴

1.1 Growth of Fintech and Digital Payments in India

India's fintech ecosystem has grown rapidly recently due to widespread adoption of digital payment technologies and technology-driven financial service providers. The fintech ecosystem includes banks, non-bank Payment System Operators (PSOs), payment aggregators, payment gateways, fintech platforms, technology providers and other players. However, fintech operators perform a diverse range of regulatory functions and hence, different legal obligations may apply to different categories of operator, depending upon which regulatory obligations are subsumed by a particular entity.⁵

¹ Payment and Settlement Systems Act, 2007, No. 51 of 2007, §§ 3–4 (India); Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators* (July 30, 2024).

² Reserve Bank of India, *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices* (Nov. 7, 2023); Reserve Bank of India, *Master Direction on Digital Payment Security Controls* (Feb. 18, 2021).

³ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, IRDAI/NL/CIR/MISC/242/09/2021 (Sept. 8, 2021); Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

⁴ Insurance Regulatory and Development Authority of India, *Guidelines on Information and Cyber Security for Insurers and Insurance Intermediaries* (2022); Reserve Bank of India, *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices*, supra note 2.

⁵ Payment and Settlement Systems Act, 2007, supra note 1; Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

The RBI's regulatory approach recognises this diversity. The Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank PSOs issued in 2024 establish requirements concerning governance, risk assessment, security controls, vendor management, data security, incident response, business continuity and digital payment security. The Directions also recognise that PSOs may depend upon payment gateways, technology vendors and other third-party service providers and therefore require them to identify and manage cyber and technology risks arising from such relationships.⁶

This regulatory structure is significant for cyber insurance because the risk profile of a fintech organisation cannot be assessed solely by examining its internal information technology infrastructure. A fintech enterprise may depend upon cloud service providers, software vendors, payment processors, application developers, telecommunications providers and other participants in the digital payment chain. Consequently, cyber insurance underwriting increasingly needs to examine the broader technology ecosystem rather than treating cyber risk as an isolated organisational risk.⁷

High-frequency and high-severity digital threats including artificial intelligence-enabled attacks, sophisticated phishing campaigns, ransomware and supply-chain compromises present rapidly evolving risks for financial technology companies. Some of these risks may affect multiple financial institutions simultaneously and may therefore create correlated losses. The changing cyber risk environment calls for specialised underwriting practices capable of assessing not only the technical security of an individual insured but also its exposure to interconnected technology infrastructure and systemic cyber events.⁸

1.2 Cyber Risk and the Need for Insurance

The coverage available under cyber liability insurance can vary depending on the specific policy. First-party coverage can include costs incurred in incident response, forensic investigations, data restoration, business interruption and certain types of cyber extortion. Third-party coverage can provide protection against claims by customers, business partners and other affected parties. Some policies may also address regulatory investigation costs and payment fraud, subject to defined conditions, exclusions and definitions.⁹

The existence of a cyber insurance policy does not however guarantee coverage for every cyber-related loss. Traditional exclusions relating to fraud, contractual liability, war, infrastructure failure or intentional acts may interact with cyber-specific provisions in complex ways. An employee-led payment fraud involving social engineering may therefore raise questions concerning whether the loss should be classified as a cyber event, employee dishonesty, financial crime or an unauthorised electronic transaction.¹⁰

This classification problem is particularly significant in fintech because a single incident may simultaneously contain technological, financial and human elements. For example, a fraudulent payment may begin with phishing, involve the disclosure of authentication credentials, result in an authorised transfer and ultimately cause a financial loss to a customer or financial institution. The question of which insurance

⁶ Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

⁷ Id.

⁸ Id.; Reserve Bank of India, *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices*, supra note 2.

⁹ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

¹⁰ Id.; see also Insurance Regulatory and Development Authority of India, *Guidelines on Information and Cyber Security for Insurers and Insurance Intermediaries*, supra note 4.

policy responds to the loss may therefore depend upon the precise wording of the policy rather than merely the factual description of the cyber incident.

Cyber Risk Insurance: Role in Risk Management



FIGURE 1. *Role of Cyber Risk Insurance in Risk Management*

2 CYBER RISKS AFFECTING FINTECH AND DIGITAL PAYMENTS

2.1 Payment Fraud and Social Engineering

Payment fraud presents significant cyber risks to digital financial services. Payment fraud incidents typically exploit social engineering tactics to coerce customers or employees into carrying out fraudulent transactions. Examples include phishing, vishing, business email compromise, impersonation and fraudulent instructions.¹¹

Policies may provide limited coverage for these risks in that the loss situation resulting from a cyber-crime attack, for instance, may be covered while loss resulting from a voluntary transfer of funds may be excluded. A more substantial provision is a social engineering coverage which clearly specifies exclusions that revolve around authentication, internal control and incident reporting requirements. These distinctions underline the importance of clear drafting in ensuring the payments and technology risks are understood.¹²

Under the RBI's regulatory framework for payment fraud prevention, payment fraud is increasingly recognized as a part of operational and cyber resilience that is worth monitoring and preventing. For example, the 2024 Directions require fraud monitoring and transaction monitoring in financial

¹¹ Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

¹² Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

institutions in addition to other regulations that recognise payment frauds as one of the many ways to identify unauthorised or fraudulent digital transactions.¹³

Cyber insurance should complement these regulatory controls. Insurers may rely upon exclusions and warranties where an insured fails to maintain required safeguards. Nevertheless there is a need to distinguish intentional or reckless non-compliance from an isolated failure that occurs despite an otherwise reasonable cybersecurity programme. The legal consequences of a cybersecurity deficiency should ideally bear a rational relationship to the loss for which indemnification is claimed.¹⁴

2.2 Data Breaches and Identity Theft

Fintech organisations process substantial quantities of personal and financial information. Customer names, identification details, account information, transaction records, authentication information and other sensitive data may be processed across several technological environments. A data breach can therefore produce consequences extending beyond the immediate cost of repairing affected systems.¹⁵

The Information Technology Act, 2000 provides an important statutory foundation for addressing unauthorised access, damage to computer systems and computer-related offences. The Digital Personal Data Protection Act, 2023 subsequently established a dedicated legislative framework concerning the processing and protection of digital personal data. For financial technology organisations the interaction between cybersecurity obligations and data protection obligations is therefore increasingly important.¹⁶

For insurers, data breach risk may include forensic investigation costs, legal costs, notification costs, crisis management, remediation costs and third party claims. Insurance policy wording may also include provisions requiring certain security measures, incident notification and cooperation with the insurer. Such provisions are likely to be especially relevant where the insured is already subject to statutory data protection and incident reporting obligations.¹⁷

The statutory privacy obligations and the insurance policy wording may, however, be based on different concepts. A statutory reporting obligation may arise where personal data has been lost, even if the insured has not itself incurred an equivalent monetary loss. On the other hand, the insured could suffer lengthy interruption as a result of a cyber incident that does not involve loss or unauthorised access to personal data. Cyber insurance may thus be rendered ineffective if all losses are treated as data breach losses.¹⁸

2.3 Ransomware and Business Interruption

Ransomware is a growing threat for highly digitised organisations. Ransomware may block an organisation's access to its systems, affect payment processing and prevent customers from requesting financial services. Thus, even if personal data has not been irretrievably lost, significant losses can still occur.¹⁹

¹³ Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

¹⁴ Id.; Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, supra note 2.

¹⁵ Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India); Information Technology Act, 2000, No. 21 of 2000 (India).

¹⁶ Information Technology Act, 2000, supra note 15; Digital Personal Data Protection Act, 2023, supra note 15.

¹⁷ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

¹⁸ Id.

¹⁹ Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

CERT-In's directions requiring reporting of cyber incidents are especially relevant in this context. The 2022 Directions under section 70B of the Information Technology Act listed defined classes of cyber incidents which must be reported within the relevant period, given the seriousness of some types of incidents, specifically including ransomware events and data breaches.²⁰

This closely links incident response and the insurance claims process. For instance, a cyber insurance policy may require prompt notification of the insurer, while the insured may also be subject to a regulatory requirement to notify CERT-In. Therefore, lack of timely reporting may be harmful under both the regulator and the insurance contract. An incident response plan should therefore combine regulatory reporting with notification to the insurer and evidence protection.²¹

Business interruption is another significant coverage issue. Loss is incurred not because the insured technological systems themselves were compromised but because a third-party service provider was blocked. Therefore, the classic line between direct and indirect losses becomes more difficult to maintain in this highly networked digital payments ecosystem.²²

2.4 Third-Party and Supply-Chain Risk

Most modern fintech firms are not standalone. Their operations rely heavily on cloud platforms, software developers, payment gateways, data centres, cybersecurity providers and other technology vendors. Thus, a cyber incident at one of these vendors can affect a number of downstream entities and customers.²³

The RBI's 2024 Directions sit squarely on vendor risk and require PSOs to analyse and manage technology and cyber risk concerning third parties. In addition, they recognise the importance of security controls in vendor environments and the need to manage critical service providers.²⁴

The above has far-reaching implications for cyber insurance. Usually, cyber policies focus on the insured's own systems. However, the source of disruption may originate in the infrastructure of a vendor. Insurance contracts therefore need to differentiate between direct cyber incidents and those stemming from third parties or supply chain attacks. Contingent business interruption is a key area of concern in this respect.²⁵

Table 1: Major Cyber Risks and Potential Cyber Insurance Responses

Cyber Risk	Potential Consequence	Possible Insurance Response	Major Coverage Issue
Phishing and social engineering	Fraudulent transfer	Cybercrime or social engineering cover	Voluntary transfer exclusions
Data breach	Privacy claims and response costs	Data breach and liability cover	Regulatory and third-party liability
Ransomware	System disruption and restoration costs	Cyber extortion and business interruption cover	Exclusions and policy conditions
Payment fraud	Direct financial loss	Payment fraud or crime extension	Authentication and internal controls

²⁰ Indian Computer Emergency Response Team, *Directions under Section 70B of the Information Technology Act, 2000*, Apr. 28, 2022.

²¹ Id.; Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

²² Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

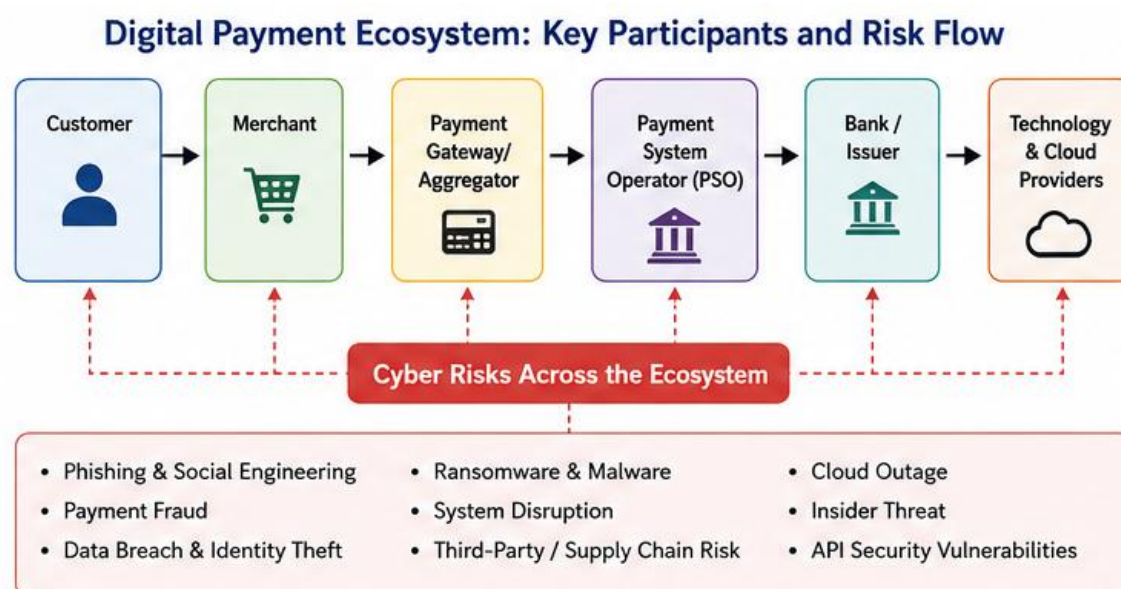
²³ Id.

²⁴ Id.

²⁵ Id.; Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

Cyber Risk	Potential Consequence	Possible Insurance Response	Major Coverage Issue
Third-party attack	Service disruption	Contingent business interruption	Causation and vendor dependency
Cloud service failure	Loss of digital services	Business interruption extension	Service provider exclusions
Regulatory investigation	Legal and compliance costs	Regulatory cover where insurable	Scope of coverage

Source: Compiled by the author based on the Indian legal and regulatory framework concerning cybersecurity, digital payments and cyber insurance.



Source: Compiled by the author.

FIGURE 2. *Digital Payment Ecosystem*

3 INDIAN LEGAL AND REGULATORY FRAMEWORK

3.1 Information Technology Act, 2000

The Information Technology Act, 2000 is one of the Indian cyber legal systems covering unauthorised access, damage to computer systems, computer insider crimes and responsibilities of intermediaries among other issues. The Act provides the statutory basis for the legal effects following a cyber risk event.²⁶

The current Indian legal framework is relevant to fintech companies beyond criminal liability. Cyber risk issues ranging from unauthorised access and damage to computer resources to data security would challenge fintech companies to evaluate the legal aspects of these risks. The Act is therefore one part of the Indian legal framework for cyber risk.²⁷

Cyber insurance does not affect existing statutory responsibilities under the IT Act. The insured party is still liable for adhering to the applicable requirements and the reporting obligations of the IT Act. Cyber

²⁶ Information Technology Act, 2000, supra note 15, §§ 43, 43A, 66.

²⁷ Id.

insurance simply allows transfer of risks related to the insured events and does not affect the current liabilities of the insured party.²⁸

3.2 Payment and Settlement Systems Act, 2007

The Payment and Settlement Systems Act, 2007 serves as the statutory basis for the regulation of payment systems by RBI. The Act duly empowers the RBI to regulate payment systems and issue directions for the same. Hence, it is important to understand the legal obligations of participants in the digital payment ecosystem in India.²⁹

The RBI's 2024 cyber resilience directives for non-bank PSOs were published under sections 10(2) and 18 of the PSS Act. They aim to bolster the cyber resilience of payment systems and institute governance and operational processes for cyber risk.³⁰

The PSS Act renders certain implications on cyber insurance underwriting. Underwriters of payment operators cannot dismiss exposures to cybersecurity as wholly voluntary risk management practices. The expected adherence in most cases may become a factor in their underwriting review.³¹

3.3 RBI Cybersecurity Framework

The RBI has increasingly imposed cybersecurity requirements on banks and payment ecosystem participants. The 2021 Master Direction on Digital Payment Security Controls set out common minimum-security requirements for covered regulated entities, covering governance, secure application development, threat modelling, security testing, logging and monitoring and secure-by-design principles.³²

The 2024 Master Directions that are applicable to non-bank PSOs go further, by combining cyber resilience with digital payment security. The Directions cover governance, risk assessment, identity and access management, network security, application security, security testing, vendor risk, data security, incident response, business continuity, cloud security, and payment fraud monitoring.³³

These can in turn serve as a helpful basis for risk-based underwriting of cyber insurance. Insurers can examine the applicant's authentication controls, monitoring systems, incident handling, backup policies, vendor management, and business continuity protocols. To be certain, however, it should be noted that regulatory requirements do not automatically constitute contractual warranties. The legal effect of a breach would be determined by the terms of the insurance contract and the manner in which those terms are drafted.³⁴

A distinction should therefore be made between regulatory compliance and insurance coverage. The application of regulatory standards may have an important role to play in risk quantification but policy wording should delineate those security requirements that are material conditions of coverage and those that offer warranties to the insurer, and the consequences that accrue to the insured on the grounds of breach of the latter.

²⁸ Id.; Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

²⁹ Payment and Settlement Systems Act, 2007, supra note 1.

³⁰ Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

³¹ Id.

³² Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, supra note 2.

³³ Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

³⁴ Id.; Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

3.4 Data Protection and CERT-In Requirements

Data protection has become an increasingly important part of cyber risk management. The Digital Personal Data Protection Act, 2023, provides a statutory framework for protecting digital personal data. The implementation of the Act is brought about through provisions on commencement and rules made thereunder.³⁵

With respect to payment services, data protection regulation is especially important to fintechs. A cyber incident can have multiple privacy, regulatory, contractual and insurance implications. In such scenarios, the insured may need to deal with customers, regulators, law enforcement, business partners and insurers because of the incident.³⁶

CERT-In requirements are an important part of the framework. The 2022 Directions issued under section 70B of the IT Act put forward requirements on cybersecurity practices and incident reporting. The official guidance from CERT-In also indicates that where all the requisite information is not available in the reporting period, the available information may be given and more information may be provided later.³⁷

Cyber insurance is therefore an important part of the event response strategy of a fintech. Insurance policies include requirements on notification, cooperation and evidence preservation. Therefore, the regulatory notification and the insurer's notification need to be carefully coordinated so that it does not prejudice the insured's regulatory position or insurance claim.³⁸

3.5 Role of IRDAI

IRDAI has a key role to play in shaping the insurance framework in which the cyber insurance product is offered. In September 2021, IRDAI issued a Product Structure for Cyber Insurance after thinking about the nature of cyber risks in development and the problem with rigid standardisation in the dynamic environment. The regulator considered that cyber risk is influenced by current legislation, advancements in technology, interconnectivity and new forms of loss.³⁹

The flexibility of this approach provides insurers with the ability to develop products according to changing cyber risks. However, too much variation in policy terminology and coverage structures can generate uncertainty for policyholders. Therefore, a fintech enterprise could find that it is difficult to compare policy coverage based solely on premium, as the scope of coverage can vary substantially among insurers.⁴⁰

A preferable solution is not necessarily a complete standardisation of all aspects of cyber insurance policy wording. Instead, India could look to implement standardised definitions for core concepts while maintaining flexibility in the additional coverage. Terms such as cyber incident, data breach, social engineering, payment fraud, business interruption, security failure and third-party service provider could be subject to minimum regulatory terminology.⁴¹

³⁵ Digital Personal Data Protection Act, 2023, *supra* note 15; Ministry of Electronics and Information Technology, *Digital Personal Data Protection Rules, 2025* (Nov. 14, 2025).

³⁶ Digital Personal Data Protection Act, 2023, *supra* note 15.

³⁷ Indian Computer Emergency Response Team, *Directions under Section 70B of the Information Technology Act, 2000*, *supra* note 20.

³⁸ *Id.*; Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, *supra* note 3.

³⁹ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, *supra* note 3.

⁴⁰ *Id.*

⁴¹ *Id.*

4 EMERGING COVERAGE GAPS

4.1 Payment Fraud and Social Engineering

The most significant and emerging coverage gap concerns the losses resulting from social engineering. As digital payment fraud becomes more sophisticated, the deception rather than the technical intrusion is often the crux of the problem. The employee may be instructed through an email that looks like it is from the senior management team or the customer may reveal his login details or authorise the transaction.⁴²

The legal position is not always clear cut. If the victim has technically authorised the transaction one could argue that it has not been unauthorised. From a commercial and pragmatic point of view, however, the transaction was based on deception. The classification of the inbound claim as cyber or crime insurance or neither depends on such a distinction.⁴³

The regulatory framework must therefore evolve to a more functional rather than technical definition. Coverage should be predicated on the type of insured event rather than on the nature and authenticity of the intrusion.⁴⁴

4.2 Regulatory Compliance and Security Warranties

Cyber policies may contain representations and warranties concerning cybersecurity controls. These may relate to multi-factor authentication, encryption, backups, patch management, privileged access controls, endpoint protection and incident response. Such provisions can assist insurers in assessing and pricing cyber risk.⁴⁵

At the same time security warranties can create uncertainty for insured organisations. A fintech enterprise may satisfy the required controls when the policy is issued but subsequently experience a technical deviation. If the warranty is drafted as an absolute condition of coverage a relatively minor breach could potentially be relied upon to deny a claim even where the breach did not materially contribute to the insured loss.⁴⁶

Insurance law places considerable importance upon the terms of the insurance contract. The Supreme Court has repeatedly allowed that the scope of insurance coverage is determined by the contractual terms and that courts must be careful to scrutinise the language of the policy when determining the insurer's liability.⁴⁷

A balanced regulatory approach should therefore require insurers to identify material cybersecurity representations clearly and explain the consequences of breach. Coverage should not automatically be removed because of a technical deviation that has no material connection with the insured loss unless the policy expressly provides for such a consequence and the term is legally enforceable.⁴⁸

⁴² Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

⁴³ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

⁴⁴ Id.

⁴⁵ Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, supra note 2; Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

⁴⁶ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

⁴⁷ *Oriental Insurance Co. Ltd. v. Sony Cheriyan*, (1999) 6 SCC 451; *United India Insurance Co. Ltd. v. Harchand Rai Chandan Lal*, (2004) 8 SCC 644.

⁴⁸ *United India Insurance Co. Ltd. v. Harchand Rai Chandan Lal*, (2004) 8 SCC 644; Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

4.3 Third-Party and Systemic Risk

A further major gap arises from third-party dependency. A fintech enterprise may maintain adequate internal cybersecurity controls and nevertheless suffer substantial loss because its cloud service provider, payment gateway or technology vendor experiences a cyber disruption.⁴⁹

The RBI's 2024 Directions recognise this interconnectedness by requiring PSOs to assess and manage risks arising from vendors and other third parties within the digital payment ecosystem. This regulatory recognition should be reflected in cyber insurance contracts through clear provisions dealing with contingent business interruption and dependent business interruption.⁵⁰

Insurance policies should specify whether the relevant third party must be an identified service provider, whether the third-party incident must satisfy the definition of a cyber event and whether geographical restrictions apply. Such clarity can reduce disputes concerning causation and the scope of insured loss.⁵¹

An even more important risk is that of systemic cyber risk. Cyber incidents that take advantage of a vulnerability present in widely used software or cloud infrastructure can result in simultaneous losses among multiple insureds, thereby creating large accumulation risk for insurers.⁵²

The risk of systemic cyber events further supports the need for catastrophe modelling, stress testing and suitable reinsurance arrangements. Very large correlated cyber events could strain insurance capacity and question the assumptions about diversification of risk.⁵³

5 INTERNATIONAL COMPARISONS

5.1 European Union

The Digital Operational Resilience Act (DORA) is an important comparative model for India. DORA sets out an elaborate regulatory framework for the provision of digital operational resilience in the financial sector. Covered agencies are required to manage risks arising from information and communications technology (ICT) use, report incidents and maintain resilience measures. DORA also sets out rules that apply to ICT third parties.⁵⁴

Adopting an integrated approach suggests that cyber risk is not strictly an information security problem but that it is also an operational and financial resilience challenge. The relevance of this approach for India is that fintech platforms are becoming increasingly integrated into the financial system.⁵⁵

DORA also emphasizes the importance of ICT third-party risk. Given the relatively limited number of technology providers upon which financial institutions rely, a disruption inflicted on one of these providers may affect more than one institution. The relevance of this principle to cyber insurance policy

⁴⁹ Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

⁵⁰ Id.

⁵¹ Id.

⁵² Id.

⁵³ Id.

⁵⁴ Regulation (EU) 2022/2554 of the European Parliament and of the Council of Dec. 14, 2022, on Digital Operational Resilience for the Financial Sector, 2022 O.J. (L 333) 1.

⁵⁵ Id.

also lies in the fact that the source of an insured's cyber exposure need not arise from within the insured's own organisational perimeter.⁵⁶

India need not copy DORA in a literal sense. However, its holistic view of digital operational resilience has implications for the future design of Indian cyber insurance regulation. Cybersecurity compliance, vendor management, incident reporting, and risk transfer via insurance act increasingly in a synergistic manner to contribute to financial resilience.⁵⁷

5.2 United States

The United States offers a divergent paradigm in which cybersecurity regulation is enforced through federal and state level requirements and sector-specific regulatory bodies. New York's cybersecurity regulation for financial services entities offers an important illustration of detailed organisational IT security satisfying requirements that apply to regulated entities.⁵⁸

The US cyber insurance market has also evolved sophisticated underwriting practices. Insurers make increasing use of detailed questionnaires, technical reviews and security information to assess the risk profile of applicants. Policies may include first-party and third-party coverages with extensions covering social engineering, business interruption, ransomware and regulation-related exposures.⁵⁹

The US experience illustrates both the merits and limits of a market-based cyber insurance regulatory framework. On the one hand, flexible underwriting may motivate ultimate policyholders to improve their security posture as robust security measures may affect the availability and pricing of coverage. On the other hand, considerable variation in policy wording can lead to uncertainty as to the precise scope of protection.⁶⁰

India could adopt a hybrid market-regulatory approach. Defining a baseline set of regulatory requirements for coverages and disclosures could permit insurers to maintain some flexibility in the design of policies tailored to different categories of risk associated with fintech and digital payments products and services.

⁵⁶ Id.

⁵⁷ Id.; Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

⁵⁸ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.

⁵⁹ Id.

⁶⁰ Id.

Comparative Regulatory Approaches to Cyber Resilience			
Aspect	India	European Union (DORA)	United States
Regulatory Nature	Sectoral (RBI, IRDAI, CERT-In, DPDP Act)	Comprehensive EU-wide framework	Sectoral + State-based (Regulatory patchwork)
Focus Areas	Cybersecurity, Payment Security, Data Protection	ICT Risk, Incident Reporting, Resilience Testing, Third-party Risk	Cybersecurity, Standards, Disclosure, State Regulations
Third-Party Risk	Addressed by RBI (2024 Directions)	Strong emphasis with direct oversight of critical ICT providers	Addressed through contracts and supervisory guidance
Incident Reporting	CERT-In (within 6 hours) + Sector Regulators	Harmonised thresholds and timelines	Varies by sector and jurisdiction
Insurance Linkage	Evolving integration with regulation	Operational resilience expected to influence insurance	Driven by market, underwriting practices
Approach	Building coordinated framework	Integrated, principles-based with prescriptive elements	Market-led with regulatory oversight

Source: Compiled by the author.

FIGURE 3. *Comparative analysis*

6 RECOMMENDATIONS FOR LEGAL AND REGULATORY REFORM

Greater consistency between insurance products and clear definitions for common terminology will be instrumental in the development of this space. IRDAI should launch a regulatory glossary which will codify minimum terms and definitions for common terms such as cyber incident, data breach, ransomware, social engineering, payment fraud, business interruption, system failure and third-party cyber event. This will enhance comparability between insurers providing cyber insurance while also allowing them freedom on policy wording.⁶¹

Underwriting decisions should become more risk-based and include a review of the Internet service provider (ISP) and hosting details supplied by the applicant. Insurers should evaluate the apposite cybersecurity measures implemented by the applicant, which should reflect the regulatory classification and risk profile of the business. The measures are expected to include but not be limited to, adherence to RBI requirements, authentication, security testing, incident response, backup, vendor management, and business continuity.⁶²

Inclusion of social engineering and payment fraud coverage in policy wording has received great attention. Insurers should be transparent on whether the fraudulent transfer caused by deception is covered and under what circumstances. This will reduce ambiguity on whether a payment fraud is covered as an unauthorized transaction, a cyber event or a crime event.⁶³

Security warranties should also be proportionate and causally connected to the insured loss. Insurers should be able to protect themselves against material cybersecurity deficiencies but a technical deviation

⁶¹ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

⁶² Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

⁶³ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

that has no meaningful relationship with the loss should not automatically result in denial of an otherwise valid claim unless the policy clearly provides for that result.⁶⁴

Third-party and supply-chain risks should receive explicit treatment. Cyber insurance policies for fintech organisations should address cloud providers, payment processors, software vendors and other critical service providers. The policy should identify when an incident originating with a vendor constitutes an insured event and whether contingent business interruption coverage applies.⁶⁵

Greater coordination between regulators is also necessary. RBI, IRDAI, CERT-In and data protection authorities have distinct institutional responsibilities but their requirements may overlap during a cyber incident. Coordination concerning incident reporting, evidence preservation, investigation, business continuity and insurance claims would reduce regulatory uncertainty and improve incident response.⁶⁶

Insurers should also develop stronger capabilities for assessing systemic cyber risk. As financial technology infrastructure becomes increasingly concentrated a single vulnerability may affect numerous organisations simultaneously. Scenario analysis, catastrophe modelling and appropriate reinsurance arrangements should therefore form an increasingly important part of cyber risk underwriting.⁶⁷

Finally, fintech organisations need to consider cyber insurance as a part of a more comprehensive cyber risk management approach. Insurance should not serve as a substitute for investments in cybersecurity measures. Organisations should establish incident response strategies that bring together technical teams, senior management, legal advisers, the regulators and insurers. This should help mitigate cyber incident impact as well as disputes over insurance coverage.⁶⁸

7 FINDINGS AND DISCUSSION

The analysis shows that the fintech and digital payments ecosystem in India is evolving while the cyber risk environment is also becoming increasingly complex. While the RBI has set out detailed cybersecurity requirements for payment system participants and the CERT-In has set out reporting obligations, the IRDAI has concurrently formulated standards for cyber insurance products. The existence of these regulatory initiatives indicates that cyber risk is now an issue that extends beyond technology and permeates financial and operational resilience.⁶⁹

The central finding of the research is that India's major challenge is not a lack of comprehensive regulations. Rather, the challenge is dealing with the fragmentation of regulations on cybersecurity, regulations on payment systems, data protection laws, and insurance laws. As a result, a fintech firm may have

⁶⁴ *United India Insurance Co. Ltd. v. Harchand Rai Chandan Lal*, (2004) 8 SCC 644.

⁶⁵ Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

⁶⁶ Indian Computer Emergency Response Team, *Directions under Section 70B of the Information Technology Act, 2000*, supra note 20; Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

⁶⁷ Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

⁶⁸ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

⁶⁹ Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1; Indian Computer Emergency Response Team, *Directions under Section 70B of the Information Technology Act, 2000*, supra note 20.

multiple obligations relating to a single cyber incident and the insurance policy may use distinct terminology and differing contractual requirements.⁷⁰

A second finding is the increasingly difficult line between cyber risk and financial crime. Social engineering is a clear example. A spoofed digital payment can be a technology-based incident, a human-enabled fraud and a financial crime simultaneously. Insurance products based on a rigid separation between these may create coverage uncertainty.⁷¹

A third finding is third-party dependency. Fintechs often use third-party technology vendors for cloud services, software development, payment systems and other critical services. Cyber insurance in the Indian context should not only evaluate the cyber risk of the insured entity but also material third-party-dependent risk.⁷²

A fourth finding is that cybersecurity compliance with regulatory requirements can become an important underwriting criterion. RBI governance, security testing, vendor risk governance, data security, incident response and business continuity requirements offer a good starting point to assess cyber risk. However, cybersecurity compliance requirements should not be automatically treated as pure and absolute insurance warranties without careful examination of causation and fairness in contractual terms.⁷³

The comparative analysis suggests that India can learn from international experience without directly copying foreign models. The EU approach demonstrates the value of integrated digital operational resilience while the US experience highlights the strengths and weaknesses of flexible market-based cyber insurance. India can incorporate these lessons while retaining a regulatory framework suited to the particular characteristics of its domestic digital payment ecosystem.⁷⁴

8 CONCLUSION

As India's fintech and digital payment ecosystem continues to grow, cyber risk insurance will become increasingly important. The scale, technological interconnectedness and speed of digital financial services mean that one cyber incident can generate losses extending well beyond the immediate technological impact. Payment fraud, social engineering, data breaches, ransomware, business interruption and third-party technology failures may generate financial, regulatory, contractual and reputational consequences simultaneously.⁷⁵

India has built essential components of a cyber risk governance structure with the Information Technology Act, 2000, Payment and Settlement Systems Act, 2007, Digital Personal Data Protection Act, 2023, RBI cyber security directions, CERT-In mandates and the IRDAI framework for cyber insurance.

⁷⁰ Information Technology Act, 2000, *supra* note 15; Payment and Settlement Systems Act, 2007, *supra* note 1; Digital Personal Data Protection Act, 2023, *supra* note 15; Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, *supra* note 3.

⁷¹ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, *supra* note 3.

⁷² Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, *supra* note 1.

⁷³ Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, *supra* note 2; Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, *supra* note 1.

⁷⁴ Regulation (EU) 2022/2554, *supra* note 54; N.Y. Comp. Codes R. & Regs. tit. 23, § 500.

⁷⁵ Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, *supra* note 1.

RBI's 2024 Master Directions are particularly noteworthy because they bind together cyber resilience and cyber risks to digital payment security and third parties.⁷⁶

Yet many gaps remain. Payment fraud and social engineering underline the challenge of separating cyber incidents from financial crimes. Security warranties can breed doubt where contract stipulations are strictly more demanding than the causal link between a cybersecurity failure and the insured loss. Third-party connectivity bears further doubt over contingent business interruption while systemic cyber events give rise to difficult issues about insurance capacity, accumulation and reinsurance.⁷⁷

Consequently, the future development of cyber risk insurance in India should concentrate on regulatory coordination. It is not about augmenting the number of regulations. Instead of merely clarifying descriptive terminology and policy disclosures, IRDAI can facilitate transparency and information disclosure facilitating decision making and lessening asymmetric information between insurers and insured. The concomitant advancements in standard-setter mechanisms such as cybersecurity best practice standards promulgated by RBI, and incident reporting obligations enforced by CERT-In, can provide enhanced foundations for the assessment of cyber risk.⁷⁸

A mature cyber insurance market in India should pursue three interlinked objectives: efficient transfer of cyber risk, enhanced incentives for better cybersecurity, and increased legal predictability. The requisite regulatory architecture must be cognisant of the fact that financial technology and cyber risk insurance share such strong interdependencies with cybersecurity best practice, payment system safeguards, and data protection norms.⁷⁹ To that end, an integrated regulatory framework that fosters consumer confidence, ensures financial system stability, and promotes sustainable growth of digital financial services can bring about subtler but more important gains for the Indian economy.

* * *

⁷⁶ Information Technology Act, 2000, supra note 15; Payment and Settlement Systems Act, 2007, supra note 1; Digital Personal Data Protection Act, 2023, supra note 15; Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1; Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3.

⁷⁷ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3; Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.

⁷⁸ Id.; Indian Computer Emergency Response Team, *Directions under Section 70B of the Information Technology Act, 2000*, supra note 20.

⁷⁹ Insurance Regulatory and Development Authority of India, *Product Structure for Cyber Insurance*, supra note 3; Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators*, supra note 1.