



A Conceptual Overview Of Cyber Insurance In India

K Kedar Gawrav¹, G L Meenaz², R Vasanthselvakumar³, Sathya Geetha Ganesan⁴

^{1,2}Department of MBA, Viswam Engineering College, Madanapalle, AP, India

³Department of CSE, Viswam Engineering College, Madanapalle, AP, India

⁴Dept. of Civil and Environmental Engineering, San Jose State Univ., 1 Washington Square, San José, CA, USA.

* Corresponding Author : Sathya Geetha Ganesan; sathuicsivan@gmail.com

Abstract: Cyber insurance is emerging as an important mechanism for managing the growing financial and operational risks associated with cyber threats in India. Rapid digitalization, cloud adoption, online transactions, and increasing dependence on information technology have exposed organizations to risks such as data breaches, ransomware, phishing, business interruption, and cyber fraud. Cyber insurance provides financial protection against selected losses arising from such incidents and can support organizations in improving their cybersecurity preparedness. This study presents a conceptual overview of cyber insurance in India, focusing on its importance, coverage, major cyber risks, benefits, and challenges. It also examines factors influencing the adoption of cyber insurance, including awareness, policy complexity, risk assessment, premium costs, regulatory requirements, and the evolving nature of cyber threats. The study highlights the need for greater awareness, standardized policy frameworks, effective risk assessment, and stronger collaboration among insurers, businesses, cybersecurity professionals, and regulators to promote a resilient cyber-risk management ecosystem in India.

Keywords: Cyber Security Insurance, Cybercrimes, Digital Payments.

1. Introduction

The rapid growth of digital technologies has transformed the way businesses, financial institutions, government organizations, and individuals operate in India. The increasing use of online banking, digital payments, cloud computing, e-commerce, and interconnected information systems has improved efficiency and accessibility. However, this digital transformation has also increased exposure to cyber threats such as ransomware, phishing, malware, identity theft, data breaches, and cyber fraud.

Such incidents can result in financial losses, operational disruptions, reputational damage, and legal or regulatory consequences. In this environment, cyber insurance has emerged as an important component of organizational risk management. Unlike traditional insurance products, cyber insurance is designed to address losses associated with digital and cyber-related incidents. Depending on the policy, coverage may include costs related to data recovery, business interruption, incident response, legal assistance, notification of affected parties, and certain third-party liabilities.

In India, the cyber-insurance market is developing alongside the country's rapidly expanding digital economy. Organizations, particularly businesses that handle large volumes of sensitive customer and financial information, are increasingly considering cyber insurance as part of their broader cybersecurity strategy. However, adoption faces several challenges, including limited awareness, difficulties in assessing cyber risk, variations in policy coverage, high or uncertain premiums, exclusions, inadequate historical loss data, and the rapidly changing nature of cyberattacks.

Therefore, understanding cyber insurance in India is important for evaluating its role in managing emerging digital risks. This study provides a conceptual overview of cyber insurance in India, examining its key features, coverage areas, benefits, challenges, and factors influencing adoption. It also emphasizes the importance of cybersecurity preparedness, effective risk assessment, regulatory awareness, and collaboration between organizations and insurers in developing a resilient cyber-risk management framework. Cyber insurance protects businesses against losses resulting from cyber-attacks, data breaches, and other cyber threats. It can cover the costs associated with data recovery, legal fees, and loss of income due to business interruption. In



addition, insurance for cyber security can provide businesses with access to expert advice and support to help them respond to and recover from a cyber-attack. They may also cover loss of income resulting from a cyber-attack, as well as the cost of repairing or replacing damaged equipment.

According to a report by the Indian Computer Emergency Response Team (CERT-In), there were over 1.16 lakh cyber security incidents reported in India between January and June 2021. This highlights the need for businesses to take proactive measures to protect themselves from cyber attacks. Digital payments businesses are also becoming targets of cyber attacks due to the sensitive nature of the data they handle. Cyber insurance can help these businesses mitigate the financial impact of such attacks and protect their reputation. It is important to note that cybersecurity insurance policies vary widely in terms of coverage and cost. Businesses should carefully evaluate their risks and choose a policy that is tailored to their specific needs. This may involve working with a cybersecurity insurance specialist who can help identify potential threats and recommend appropriate coverage.

Overall, insurance for cyber security can be an important tool for digital payments businesses in India to protect themselves against the financial and reputational damage taking proactive steps to prevent attacks, businesses can ensure they are well-prepared to handle the evolving threat landscape.

Coverage Options of Cyber Insurance for Digital Payment Businesses:

Digital payments businesses in India face a wide range of cyber threats, from data breaches and phishing attacks to ransomware and other forms of malware. To protect against these risks, many companies are turning to cyber security insurance. Here are some of the coverage options available:

First-Party Coverage: First-party coverage protects against losses suffered by the insured business itself. This might include:

- Data recovery costs
- Business interruption losses
- Cyber extortion payments
- Notification and credit monitoring expenses
- Public relations and crisis management costs

Third-Party Coverage: Third-party coverage protects against losses suffered by customers, partners, or other third parties as a result of a cyber incident. This might include:

- Liability for data breaches or other cyber incidents
- Costs of defending against lawsuits or regulatory actions
- Fines and penalties imposed by regulators

It's important to note that cyber security insurance policies can vary widely in terms of coverage, exclusions, and limits. Businesses should carefully review policy terms and work with an experienced insurance broker to find the right coverage for their needs.

Importance of Cyber Insurance in India for Digital Payments: Here are some reasons highlighting the importance of cyber insurance for digital payments businesses in India:

- (a) **Financial Protection:** Cybersecurity insurance provides financial protection against losses resulting from cyberattacks, data breaches, and other cyber incidents. This is particularly important for digital payments businesses that handle sensitive financial information, as a cyberattack could lead to significant financial losses.
- (b) **Reputation Management:** A cyber incident, such as a data breach, can damage the reputation of a digital payments business. Cybersecurity insurance often covers the costs associated with public relations efforts to manage and repair the company's reputation after a cyberattack, helping to regain customer trust.
- (c) **Business Continuity:** Cybersecurity insurance can cover the costs of business interruption and help digital payments businesses recover quickly after a cyber incident. This is crucial for maintaining operational continuity and minimizing the impact on business operations.
- (d) **Third-Party Liability:** Digital payments businesses often rely on various third-party service providers. Cybersecurity insurance can cover liabilities arising from breaches in third-party systems, ensuring that the business is not held solely responsible for incidents outside its direct control.
- (e) **Cyber Extortion and Ransomware Protection:** Some cybersecurity insurance policies provide coverage for cyber extortion and ransomware attacks. This coverage can assist businesses in negotiating with cybercriminals and covering ransom payments, helping to resolve such incidents with minimal impact.
- (f) **Incident Response and Forensics:** Cyber insurance often includes coverage for incident response and forensic investigations. This is essential for quickly identifying the cause of a cyber incident, implementing corrective measures, and preventing future occurrences.

Claim Process and Settlement in a Cyber India Insurance Policy for Digital Payments:

In the event of a cyber attack or data breach, having cyber security insurance can help mitigate the financial losses and reputational damage that a digital payments business may face. However, it is important to understand the claim

process and settlement procedures to ensure a smooth and efficient experience.

The first step is to notify the insurance provider of the incident as soon as possible. This can typically be done through a dedicated hotline or online portal. The insurer will then assign a claims adjuster who will work with the business to gather all necessary information and documentation. Once the claim is submitted, the insurer will conduct an investigation to determine the cause and extent of the breach, as well as the amount of damages incurred. This may involve hiring third-party experts such as forensic investigators or legal counsel.

If the claim is approved, the insurer will provide compensation in accordance with the policy terms and conditions. This may include reimbursement for expenses such as legal fees, data recovery costs, and lost income due to business interruption. It is important to note that the claim process can vary depending on the specific policy and insurer. Some policies may have specific requirements or exclusions that may affect the claim settlement. Therefore, it is crucial to carefully review the policy terms and conditions before purchasing cyber security insurance.

Selecting the Right Insurance Provider: Selecting the right insurance provider is crucial for digital payments businesses in India to ensure they have adequate coverage in case of a cyber-attack. Here are some factors to consider when selecting an insurance provider:

- (a) **Coverage:** It is important to ensure that the policy covers all the risks that the business may face, including third-party liability, business interruption, and loss of data. The policy should also cover the costs of investigations, legal fees, and public relations expenses.
- (b) **Reputation:** The reputation of the insurance provider is also an important factor to consider. The business should research the provider's history of paying claims and their overall financial stability.
- (c) **Customization:** The insurance policy should be customized to meet the specific needs of the digital payments business. This includes understanding the types of data the business handles, the potential risks, and the level of coverage required.
- (d) **Cost:** The cost of the insurance policy should also be considered. The business should compare quotes from different providers to ensure they are getting a competitive price for the coverage they need.

2. Literature Review

Cyber insurance has emerged as an important risk-transfer mechanism in response to the increasing dependence of

organizations on digital technologies. Existing research indicates that cyber insurance can help organizations manage the financial consequences of cyber incidents while encouraging better cybersecurity practices. However, the cyber-insurance market continues to face challenges related to risk assessment, underwriting, pricing, policy coverage, and limited historical data.

Marotta et al. (2017) conducted a comprehensive survey of cyber-insurance research and identified the unique characteristics of cyber risks compared with traditional insurance risks. Their study highlighted difficulties in assessing cyber risk, estimating potential losses, and developing suitable insurance products.

Tsohou et al. (2023) reviewed developments and future directions in cyber insurance and reported that the market is characterized by complex underwriting procedures, concentration among larger customers, and an imbalance between insurance demand and available capacity. The study also identified challenges in accurately assessing cyber risks and determining appropriate compensation.

In the Indian context, Deloitte (2023) examined cyber insurance through a survey of Chief Information Security Officers from India-based organizations. The study identified challenges involving technical ambiguity, difficulties in pricing cyber-risk coverage, and uncertainty regarding the responsibilities of organizations and insurers.

Recent research by Kumar et al. (2026) specifically investigated barriers and drivers influencing personal cyber-insurance adoption in India. The study identified limited understanding of cyber risks, policy complexity, and misconceptions about cybersecurity responsibilities as important barriers. It also found that awareness initiatives, media coverage, and perceived dependence on digital technologies can encourage adoption.

The regulatory environment is another important area of research. The Insurance Regulatory and Development Authority of India (IRDAI) has established information and cybersecurity guidelines for insurers and extended their applicability to insurance intermediaries, demonstrating the increasing importance of cybersecurity governance within the insurance sector.

The literature shows that cyber insurance can provide financial protection and support organizational cyber-risk management, but significant gaps remain in standardized risk assessment, transparent policy structures, pricing methodologies, consumer awareness, and India-specific empirical research. Further research is therefore needed to understand how cyber insurance can be effectively integrated with cybersecurity practices and regulatory frameworks in India.



3. Related Research Work

Several studies have examined cyber insurance from different perspectives, including risk management, insurance adoption, underwriting, pricing, and cybersecurity. These studies provide a foundation for understanding the development of cyber insurance and its relevance to the Indian context.

Marotta et al. (2017) conducted a comprehensive survey of cyber insurance research and practice. Their study examined the basic concepts of cyber insurance, its role in risk management, technological risks, and the challenges associated with developing a mature cyber-insurance market. The researchers identified issues such as limited historical data, difficulty in assessing cyber risk, and uncertainty in estimating potential losses as important research challenges.

Tsohou et al. (2023) reviewed the state of cyber insurance and identified major trends in the field. Their research examined cyber-insurance policies, underwriting, claims management, and information-security requirements. The study found that the market faces complex and lengthy underwriting processes, unclear coverage boundaries, and an imbalance between demand for insurance and available market capacity.

Palsson et al. and related research presented in The Geneva Papers (2020) examined cyber-insurance demand, supply, contracts, and cyber-loss events. The research highlighted the lack of reliable historical cyber-loss data as a major difficulty for insurers and researchers. The dynamic nature of cyber threats also makes it difficult to use historical experience as a direct indicator of future losses.

Dambra, Bilge, and Balzarotti (2020) investigated technical challenges associated with cyber insurance and proposed research directions for improving cybersecurity risk assessment. Their work emphasizes that effective cyber insurance requires better understanding of cyber vulnerabilities and the relationship between security controls and potential losses. Their research is particularly relevant to the development of technically informed underwriting practices.

Recent Indian research has focused specifically on cyber-insurance adoption. A 2026 study by Kumar et al. examined barriers and drivers influencing personal cyber-insurance adoption in India using expert interviews, surveys, and the DEMATEL technique. The study identified limited understanding of cyber risks, policy complexity, and misconceptions about cybersecurity responsibility as important barriers. It also identified educational initiatives, media coverage, and awareness of digital dependence as factors that can encourage adoption.

A separate 2026 mixed-method study by Banerjee and Das examined individual-level adoption of cyber insurance. The research developed a contextualized model to investigate factors influencing individuals' decisions to adopt cyber insurance, reflecting the growing academic interest in consumer-level cyber-risk protection. The existing research demonstrates that cyber insurance can complement cybersecurity controls by transferring part of the financial consequences of cyber incidents. However, risk quantification, limited historical data, policy complexity, underwriting difficulties, pricing uncertainty, and low awareness remain important challenges. Research specifically focused on India is comparatively emerging, creating opportunities for further studies on consumer awareness, organizational adoption, policy coverage, regulatory development, and effective cyber-risk assessment in the Indian insurance market.

(a) **How do cyber insurance policies protect against financial losses due to data breaches in payment systems?**

Cyber insurance policies for digital payment firms may offer coverage for financial losses caused by data breaches in payment systems. This may include the costs associated with investigating the breach, notifying affected customers, and providing credit monitoring services. Additionally, some policies may offer coverage for legal expenses and fines imposed by regulatory authorities.

(b) **What criteria determine the premiums for cyber security insurance in the digital payments sector?**

The premiums for cyber security insurance in the digital payments sector are typically determined based on several factors, including the size and nature of the business, the level of cyber risk exposure, the security measures in place, and the history of cyber incidents. The premiums may also vary depending on the specific coverage and limits offered by the policy.

(c) **How does cyber insurance support businesses in the event of operational disruptions caused by cyber attacks?**

Cyber insurance policies for digital payment firms may offer coverage for business interruption caused by cyber-attacks. This may include the costs associated with restoring the systems and data, and the loss of income due to the disruption. However, the coverage may be subject to certain limitations and exclusions, and may not cover all types of operational disruptions.

(d) **Can cyber security insurance provide coverage for third-party liabilities arising from digital transaction processing?**

Cyber security insurance policies for digital payment firms may offer coverage for third-party

liabilities arising from digital transaction processing. This may include the costs associated with defending against legal claims, settling lawsuits, and paying damages to affected parties. However, the coverage may be subject to certain limitations and exclusions, and may not cover all types of third-party liabilities.

(e) *What is the claims process for cyber insurance in the context of digital payment fraud?*

The claims process for cyber insurance in the context of digital payment fraud may vary depending on the policy terms and conditions. Generally, the policyholder is required to notify the insurer of the fraud and provide evidence of the loss. The insurer may then investigate the claim and determine the coverage and amount of compensation. However, the claims process may be subject to certain limitations and exclusions, and may not cover all types of digital payment fraud.

4. Conclusion

Cyber insurance is becoming an increasingly important component of cybersecurity and risk-management strategies in India. The rapid growth of digital payments, e-commerce, cloud computing, online services, and interconnected information systems has increased organizations' exposure to cyber threats such as ransomware, phishing, data breaches, malware, and cyber fraud. Cyber insurance can help organizations manage the financial consequences of such incidents and support recovery after a cyberattack.

However, the development of the cyber-insurance market in India faces several challenges. These include limited awareness, difficulties in accurately assessing cyber risks, lack of sufficient historical loss data, complex policy conditions, uncertainty in premium pricing, and the continuously evolving nature of cyber threats. Effective cyber insurance also depends on organizations maintaining appropriate cybersecurity controls and providing reliable information for risk assessment.

The study concludes that cyber insurance should complement, rather than replace, strong cybersecurity practices. Greater awareness among businesses and individuals, improved risk-assessment techniques, clearer policy structures, effective regulatory oversight, and collaboration between insurers and cybersecurity professionals can support the development of a stronger cyber-insurance ecosystem in India. As digital risks continue to evolve, continued research and innovation will be essential for making cyber insurance more accessible, transparent, and effective.

References

- [1]. Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, 24, 35–61. <https://doi.org/10.1016/j.cosrev.2017.01.001>
- [2]. Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber insurance: State of the art, trends and future directions. *International Journal of Information Security*, 22, 737–748. <https://doi.org/10.1007/s10207-023-00660-8>
- [3]. Dambra, S., Bilge, L., & Balzarotti, D. (2020). SoK: Cyber insurance? Technical challenges and a system security roadmap. *2020 IEEE Symposium on Security and Privacy*, 1367–1383.
- [4]. Aziz, B. (2020). A systematic literature review of cyber insurance challenges. *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, 357–363.
- [5]. Kumar, et al. (2026). Barriers and drivers to the adoption of personal cyber insurance in India: A DEMATEL approach. *Information and Computer Security*, 34(1), 141–169. <https://doi.org/10.1108/ICS-12-2024-0315>
- [6]. Banerjee, S., & Das, S. (2026). Cyber insurance adoption at individual level: A mixed method study. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-026-10703-9>
- [7]. Mishra, M. (2025). *An analytical study of the evolution of cyber insurance in India: Addressing coverage gaps in cybercrime and data breaches* [LL.M. dissertation]. National Law University and Judicial Academy, Assam.
- [8]. Insurance Regulatory and Development Authority of India (IRDAI). (2017). *Guidelines on Information and Cyber Security for insurers*. IRDAI/IT/GDL/MISC/082/04/2017.
- [9]. Insurance Regulatory and Development Authority of India (IRDAI). (2022). *Guidelines on Information and Cyber Security*. IRDAI/GA&HR/GDL/MISC/184/09/2022.
- [10]. Insurance Regulatory and Development Authority of India (IRDAI). (2023). *IRDAI Information and Cyber Security Guidelines*, 2023. IRDAI/GA&HR/GDL/MISC/88/04/2023.

How to Cite:

K Kedar Gawrav , G L Meenaz , R Vasanthselvakumar , Sathya Geetha Ganesan , “ A Conceptual Overview Of Cyber Insurance In India ” , International Journal of Computational Science and Engineering Research (IJCSE-R), Volume. 2, Issue. 2, p. 54 - 59 June 2025. CrossRef DOI: <https://doi.org/10.63328/IJCSE-RV2RI2P8>

Declaration

Conflicts of Interest: The authors declare no conflict of interest.

Author Contribution: All authors wrote the main manuscript text and also consent to the submission.

Ethical approval: Not applicable.

Consent to Participate: All authors consent to participate.

Funding: Not applicable, and No funding was received

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Personal Statement: We declare with our best of knowledge that this research work is purely Original Work and No third party material used in this article drafting. If any such kind material found in further online publication, we are responsible only for any judicial and copyright issues.

Generative AI Statement: The authors declare that generative AI was not used in the preparation or creation of this manuscript. The alternative text (alt text) accompanying the figures in this article was generated by Frontiers with the assistance of artificial intelligence. Reasonable efforts have been made to ensure the accuracy and appropriateness of the generated alt text, including review by the authors wherever possible. If you identify any inaccuracies or issues, please contact the editorial team.

Publisher's Note: The statements, opinions, and claims presented in this article are exclusively those of the authors and do not necessarily reflect the views of their affiliated institutions, the publisher, editors, or reviewers. Any products discussed or evaluated, as well as any claims made by their manufacturers, are not warranted, approved, or endorsed by the publisher.

Acknowledgements

We thank everyone who inspired our work