International Journal of Financial Management and Economics

P-ISSN: 2617-9210
E-ISSN: 2617-9229
IJFME 2025; 8(2): 952-962
www.theeconomicsjournal.com
Received: 26-08-2025
Accepted: 27-09-2025

Dr. Jyotirmoy Koley
Assistant Professor of Commerce, Darjeeling Government College, Darjeeling, West Bengal, India

Corresponding Author:
Dr. Jyotirmoy Koley
Assistant Professor of Commerce, Darjeeling Government College, Darjeeling, West Bengal, India

Emerging trends and challenges in India's cyber insurance sector: A multifaceted examination

Jyotirmoy Koley

DOI: https://www.doi.org/10.33545/26179210.2025.v8.i2.624

Abstract
The cyber insurance market in India is rapidly evolving, propelled by increasing digitalization and the escalating frequency and sophistication of cyber threats. Nevertheless, this emerging market faces substantial challenges that impede its growth and efficacy. This study aims to provide a comprehensive overview of the cyber insurance landscape in India, examining its evolution, current market dynamics, and prospective trends. This research employs a descriptive and analytical methodology, deriving insights from secondary data sources such as regulatory circulars, industry reports, academic literature, and news articles. The findings indicate that a lack of awareness and understanding among businesses, complexities in pricing and underwriting, non-standardized policies, and the dynamic nature of cyber risks constitute major impediments to the adoption of cyber insurance in India. This study further underscores the pivotal role of the Insurance Regulatory and Development Authority of India (IRDAI) in shaping the regulatory framework and its interaction with data privacy laws. Additionally, the study identifies key market growth drivers, including the rising costs of cybercrime, technological advancements, and the competitive advantage of insurers with cyber risk expertise. The current market landscape is characterized by the prevalence of standalone cyber policies and silent cyber or add-on covers, with standard coverage features encompassing first-party costs and third-party liabilities. Case studies of a ransomware attack on an Indian manufacturing SME and a data breach at an Indian FinTech startup provide practical insights into the role of cyber insurance in mitigating financial losses and supporting recovery efforts. This study also explores future trends, such as product innovation, increased partnerships between insurers and cybersecurity firms, and the integration of artificial intelligence into underwriting processes. Based on these findings, this study offers recommendations for stakeholders, including regulators, insurers, and businesses, to collaboratively address the challenges and foster a robust cyber insurance market in India. As cyber risks continue to evolve, the development of a comprehensive and adaptive cyber insurance ecosystem will be crucial in strengthening the resilience of Indian organizations against potential threats.

Keywords: Cyber insurance, India, challenges, regulatory framework, policy coverage, risk assessment, cybersecurity, etc.

1. Introduction
Cyber insurance is increasingly essential for risk management and mitigating the financial impact of cyber incidents. In India, the evolving digital landscape and cyber threats have increased the demand for insurance. This insurance transfers cyber risks, which is crucial for businesses in a nation with rapid digital adoption and vulnerabilities (Nurse *et al*., 2020) [25]. However, cyber insurance in India remains nascent, facing challenges such as limited data availability and regulatory advancement. The market must adapt to technological advancements and existing limitations in understanding coverage and pricing (Cremer *et al*., 2024; Marotta *et al*., 2017) [7, 23]. While cyber insurance encourages preventative measures to reduce cyber-attacks (Zhang *et al*., 2017) [41], evidence suggests that it has not effectively influenced pre-breach security in India (Arce *et al*., 2024) [4]. Understanding the mechanisms influencing India's cyber insurance landscape, including regulatory impacts and policy structuring, is crucial. Global studies suggest that cyber risk heterogeneity necessitates systematic approaches tailored to local market conditions (Khalili *et al*., 2018; Xie *et al*., 2020) [17, 40], offering valuable insights into potential growth directions in this field.

2. The Digital India Paradox

Despite its growing importance in managing cyber risks, cyber insurance in India faces several challenges. The market's nascent stage is characterized by uncertainty and a lack of standardization (Cremer, Murphy, *et al*., 2024; Marotta *et al*., 2017) [7, 23]. Policies show variability in coverage and exclusions, with insurers using ambiguous language, particularly for cyber warfare exclusions (Cremer, Fortmann, *et al*. 2024) [7]. Inadequate and fragmented data in underwriting and claims processes hinder accurate risk assessment (Nurse *et al*., 2020) [25]. The unique characteristics of cyber risks, including heavy tails and dependencies, create challenges in meeting regulatory expectations (Eling & Schnell, 2019) [12]. While cyber insurance transfers risk, it has a limited impact on improving pre-breach security levels, mainly focusing on indemnifying breach costs (Arce *et al*., 2024) [4]. The market lacks data sharing and standardized databases that are essential for collective risk management (Cremer *et al*., 2022) [8]. However, insurers are emerging as de facto regulators by requiring cyber hygiene standards (Camillo, 2017) [6], and security pre-screening could help customize policies and improve security measures (Khalili *et al*., 2018) [17].

3. Limitations of Traditional Security

Traditional security measures have several problems, especially in the context of cyber insurance in India. Cyber threats change quickly, and these old methods often cannot protect digital assets effectively. One major problem is that they cannot handle new and complex cyber threats, making them less effective in protecting organizations from all possible risks (Katiyar *et al*., 2024) [16]. In addition, traditional security is mostly reactive, dealing with threats only after they occur. This is insufficient for cyber insurance, which must manage risks before they become real problems. Vague insurance terms and unclear policy language can also cause coverage issues, making risk management more difficult (Wrede *et al*., 2020) [39]. Moreover, traditional security does not support ongoing communication between insurers and customers, which is required to update policy terms and premiums in real time. Cyber insurance requires a flexible approach to keep up with the changing security environment, which traditional models struggle with (Lepoint *et al*., 2018) [22]. In short, traditional security is limited because it is static, reactive, and cannot fully handle modern cyber threats.

4. The Digital India Initiative and Its Cyber Risk Implications

The Digital India Initiative aims to transform India into a digital society and economy. However, this change has increased cyber risks, affecting India's cyber insurance market. The increasing number of people using the Internet has increased the risk of cyber threats. As the digital world grows, more businesses and people want cyber insurance for protection against cyberattacks. Cyber insurance in India is still new compared to other countries, but the Digital India Initiative is helping it to grow. Small and medium-sized businesses (SMEs) are at risk because they have fewer resources and less cybersecurity knowledge than larger organizations. They see cyber insurance as important for managing risks as they go digital (Taskin *et al*., 2025) [35]. As cyber threats change, so does the cyber insurance market. Insurance companies are using new technologies, such as blockchain and smart contracts, to solve problems such as data transparency and fake claims (Farao *et al*., 2023) [13]. However, the market faces challenges, such as a lack of standard data, making it difficult to assess and price cyber risks accurately (Cremer *et al*., 2022) [8]. Overall, the Digital India Initiative is expected to increase the demand for cyber insurance as more people and companies become aware of the cyber risks. To meet this demand, better data management and open databases are required to improve risk assessment and policy options.

5. The Imperative for Cyber Insurance

Cyber insurance in India is growing for several important reasons. As cyber-attacks occur more often and cost more, businesses in India see cyber insurance as a key part of their risk management plans (Nurse *et al*., 2020) [25]. One of the main reasons for this insurance is the rising cost of cybercrimes. Worldwide, cybercrime costs nearly USD 1 trillion in 2020, and claims are increasing (Cremer *et al*., 2022) [8]. In India, businesses face more risks from advanced cyber threats; therefore, they need strong insurance to cover possible financial losses. However, the cyber insurance market in India is still developing and faces many challenges. These include insufficient data, no standard policies, and a lack of understanding of risks among stakeholders (Cremer, Fortmann, *et al*., 2024) [9]. Studies have shown that unclear policy terms and coverage issues are significant problems for insurers and policyholders (Cremer, Murphy, *et al*., 2024) [9]. In addition, new technologies such as cloud computing bring new risks; therefore, cyber insurance must evolve with these changes. The transition to cloud-based systems has increased risks for insurers, necessitating better insurance plans to address these challenges (Gurjar, 2025) [14]. To help the cyber insurance market grow in India, better data analysis, a deeper understanding of cyber risks, and reliable risk assessment methods are required (Palsson *et al*., 2020) [27]. The use of technologies such as blockchain and AI may solve some market problems, such as preventing fraud and expediting claims (Farao *et al*., 2023) [13]. Cyber insurance is becoming essential for businesses in India, acting as both financial protection and a strategy for managing cyber risks (Lau *et al*., 2021) [11]. As people become more aware of cyber risks, the demand for good cyber insurance will grow.

6. Problem Statement

Cyber insurance in India is vital for business risk management, but it faces challenges due to its early development stage in India. The lack of comprehensive data and standardized models hinders risk assessment and premium determinations. Evolving cyber threats complicate coverage, leading to security gaps and economic uncertainty (Cremer, Fortmann, *et al*., 2024; Nurse *et al*., 2020) [9, 25]. Unclear policy wording and exclusions create coverage gaps (Cremer *et al*., 2024) [9]. The limited understanding of cyber insurance among Indian businesses affects market development, while the global nature of cyber risks requires data pooling and public-private collaboration (Cremer *et al*., 2022; Eling & Schnell, 2016) [8, 11]. Solutions include developing standardized data collection frameworks, improved risk modelling, and policies aligned with emerging threats to create a robust cyber insurance market that enhances organizational security (Cremer, Murphy, *et*

al., 2024; Marotta *et al*., 2017) [9, 23].

7. Literature Review

Numerous scholarly articles have been authored by researchers examining various aspects of cyber insurance in India and internationally. The most significant of these articles is reviewed in this study and is presented below.

Kumar and Singh (2023) [20] presented an overview of cyber insurance in India. AIG introduced cyber insurance in 1997, and the IRDAI initiated efforts in this domain in 2019, establishing a working group in 2020. Cybercrime cases in India increased from 21,796 in 2017 to 52,974 in 2021, with fraud accounting for 60% of the cases. Cyber insurance protects businesses against financial losses from cyber-attacks, including data breaches, attacks, human error, and business disruptions. The two main types are personal cyber security insurance and corporate cyber liability insurance plans. Market growth is driven by increased digital payments, cyberattacks, and the number of Internet users. Challenges include low awareness, limited coverage, risk assessment difficulties, and high premiums for small businesses. India's emerging cyber insurance market requires increased awareness and affordable products.

Adarsh and Patil (2017) [1] investigated cyber liability insurance in the Indian e-commerce infrastructure, focusing on the banking and financial services sectors. This study highlights the digitalization of Indian banking and the rising cybersecurity threats, with banks being the primary targets because of their customer databases. The authors emphasize the need for cybersecurity policies and dispute resolution mechanisms and recommend cyber insurance as a provisional safeguard. Given the limited availability of cyber insurance in India, they recommend mandatory data breach notifications to the RBI, adoption of IT Act 2000 cybersecurity practices, and industry knowledge sharing. Although cyber insurance provides risk transfer, it does not directly mitigate risk. This study examines whether cyber insurance promotes cybersecurity best practices by analyzing insurance application forms against three standards: ISO 27001, the NIST Cybersecurity Framework, and the UK's Cyber Essentials scheme.

Adriko and Nurse (2024) [2] analyzed 68 cyber insurance application forms from US, UK, and Australian insurers from 2016 to 2023, mapping questions to controls in three security standards. Their findings show partial alignment between insurance forms and control standards, with the best practice standards underrepresented. Forms emphasize technical controls over procedural ones and focus on prevention rather than response. The UK Cyber Essentials scheme showed the strongest alignment because of its focused scope. The study reveals that while cyber insurance promotes some security best practices, gaps exist in terms of incident response and recovery. This research informs policymakers, security professionals, and insurers about the relationship between cyber insurance and security standards.

Anu (2023) [3] examined cyber insurance, which indemnifies against losses from cyberattacks and data breaches involving customer information. The coverage includes identity theft, cyberstalking, malware attacks, phishing, email spoofing, media liability claims, cyberextortion, and privacy breaches. However, it excludes intellectual property infringement, physical harm, mechanical failure, illegal activities, and cryptocurrency losses. This paper discusses Indian cybersecurity initiatives such as CERT-In, Cyber Surakshit Bharat, and the National Cyber Security Strategy 2020. Originating in 1997, the importance of cyber insurance has grown with increased technology use. The global market is expected to expand substantially in the future. This study reviews India's Information Technology Act, 2000, and cyber insurance claim procedures, which require filing an FIR, notifying insurers, and providing evidence. It concludes by emphasizing the growing role of cyber insurance in protecting against digital threats.

Singh (2024) [33] examines the effects of technological advancements on insurance, focusing on cyber insurance in India. This study highlights society's increasing reliance on IT infrastructure, intensified by COVID-19, leading to more cyberattacks and higher demand for cyber insurance. This study traces the evolution of cyber insurance from the 1970s, noting key events such as the first technology E&O policies and the Dotcom crash's impact. The study shows how the Internet of Things, blockchain, and AI are transforming insurance, enabling insurers to access databases and offer personalized products. It identifies challenges, including companies' reluctance to invest due to existing cybersecurity infrastructure, risk assessment difficulties, and policy coverage ambiguity. This study reviews India's cybersecurity laws, including the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, alongside the roles of regulatory bodies. This paper concludes by discussing cyber insurance trends, including market growth potential and new market entrants. Overall, it provides a comprehensive analysis of India's cyber insurance landscape, addressing its evolution, challenges, legal framework, and future prospects.

Taskin *et al*. (2025) [35] investigated cyber insurance adoption determinants among Turkish SMEs and their impact on digitalization. Using the TOE-I framework, they analyzed data from 168 SMEs in the Philippines. The results show that top management support, external pressures, and owner innovativeness positively influence cyber insurance adoption intention. This intention positively affects ICT adoption and organizational security performance, with ICT adoption as a mediator. Cyber insurance facilitates secure digitalization by mitigating the risks of cyberattacks. The study provides insights into SME cybersecurity strategies, although limited by single-country data, and contributes to understanding digitalization costs and benefits.

Routaray *et al*. (2024) [32] examined the significance of cyber insurance in addressing cyber-attacks. Although cyberspace has enhanced connectivity, it has introduced new vulnerabilities. Cyber incidents have increased since the pandemic and the adoption of remote work. This paper outlines cyber-attacks, including phishing, malware, and denial-of-service attacks. Cyber insurance mitigates losses from data breaches and cyber incidents. The cyber insurance market faces challenges, such as insufficient historical data and complex risk assessments. Low awareness and cumbersome processes deter potential buyers from purchasing EVs. As cybersecurity evolves, insurance will play a key role in developing cyber culture and resilience in the field. This study emphasizes the need for better implementation of cyber insurance to combat cyber-attacks in the digital world.

Kumar *et al*. (2016) [19] examine Cyber Risk Insurance (CRI) in India, highlighting the 173% increase in cybercrime cases since 2010. This study explores CRI adoption, coverage, growth barriers, and solutions through

industry interviews and report analysis. This study traces the CRI evolution from the RBI's 2001 guidelines, noting low adoption despite increasing threats. It outlines first- and third-party coverage types and IT assets covered under the CRI. The research identifies challenges, including the lack of historical data, risk prediction difficulties, and the absence of standardized metrics. Companies face barriers such as high costs, low awareness, and unclear policy scopes. This study addresses premium calculation complexities and fraudulent claim detection, suggesting predictive analytics as a solution. The authors forecast CRI market growth in India, particularly with potential government mandates for handling sensitive data. They emphasized the need for cybersecurity infrastructure while highlighting the requirements for improved awareness, policy frameworks, and risk assessment techniques.

8. Research Gap

There are many gaps in the research on cyber insurance in India. We do not know much about its effectiveness, the number of people who use it, or how it helps improve cybersecurity. Small and medium-sized businesses face challenges in using cyber insurance, but these have not been well studied. We also lack research on how Indian cybersecurity laws affect the insurance market and how cyber insurance can increase security awareness in businesses. There are not enough studies on how cyber insurance affects business resilience over time. Further research on risk assessment methods specific to India is required. The idea of public-private partnerships to boost cyber insurance use has not been well explored. We also need more studies comparing India with other growing economies and using new technologies in cyber risk assessment in India.

9. Rationale of the Study

The rationale for studying India's cyber insurance landscape stems from its unique challenges and potential benefits. Cyber insurance enables businesses to transfer risks and recover from cyber incidents (Nurse *et al*., 2020) [25]. As India's digital economy grows, companies face increasing cybersecurity threats, necessitating effective risk mitigation strategies. The nascent cyber insurance market faces developmental challenges (Marotta *et al*., 2017) [23], including insurability limitations due to insufficient data and modelling approaches (Eling & Schnell, 2016) [11]. Data availability is a significant problem for stakeholders managing cyber risks (Cremer *et al*., 2022) [8]. The Indian market shows growth potential but faces hurdles in policy standardization with unclear coverage and exclusions (Cremer *et al*., 2024) [8]. Public-private partnerships and data pooling can provide solutions for managing cyber risks in India (Eling & Schnell, 2016) [11]. This study aims to bridge these knowledge gaps, improve risk management, and facilitate better policymaking and business strategies. This research will evaluate existing insurance policies and identify improvements to enhance stakeholder resilience against cyber threats (Cremer *et al*., 2024) [8].

10. Objectives of the Study

The objectives of the present study are as follows: (i) to trace the evolution and regulatory framework of cyber insurance in India; (ii) to analyse the current market size, key players, and product offerings; (iii) to identify the major challenges hindering the adoption and growth of cyber insurance; and (iv) to discuss the future outlook and provide recommendations for market development.

11. Research Methodology

This study employed a descriptive and analytical research design. Data collection methods included the acquisition of secondary data from IRDAI circulars, annual reports of insurance companies, industry publications (e.g., from the Data Security Council of India), news articles, and academic articles, papers, and journals. Data analysis involved thematic analysis to identify key trends, challenges, and opportunities from the collected data.

12. The Indian Cyber Insurance Market: Evolution and Regulatory Framework

This section is organized into four distinct subsections: Historical Context, The Role of the Regulator (IRDAI), The Interplay with Data Privacy Law, and Market Growth Drivers. Each of these subsections is discussed in detail in the following sections.

12.1 Historical Context

The historical context of the evolution of the Indian cyber insurance market and its regulatory framework encompasses several significant developments.

1. **Emergence of Cyber Insurance**: Cyber insurance has emerged as an essential instrument for managing the risks associated with the increasing frequency and sophistication of cyberattacks. Initially conceptualized as a theoretical method of risk transfer, it has progressively evolved into a practical solution to address previously unmet needs in cyber-risk management (Marotta *et al*., 2017) [23].
2. **Challenges in Development**: The cyber insurance market faces distinct challenges, including insufficient data for risk assessment and pricing, the absence of standardized policy frameworks, and the rapid evolution of cyber threats that challenge the adequacy of existing coverage options (Lepoint *et al*., 2018; Marotta *et al*., 2017) [22, 23].
3. **Growth and Technological Integration**: Notwithstanding these challenges, the market has experienced substantial growth, primarily driven by the integration of technologies such as blockchain technology. This integration enhances transparency, automates processes, and improves customer identification systems, thereby addressing issues related to data transparency and fraudulent claims (Farao *et al*., 2023; Lepoint *et al*., 2018) [13, 22].
4. **Role of Data in Cyber Insurance**: Underwriting and claims management in cyber insurance are predominantly dependent on extensive data analysis. However, acquiring pertinent data is a significant challenge because of the ever-evolving threat landscape and variability in the security measures implemented by insured entities (Nurse *et al*., 2020) [25].
5. **Policy and Regulation**: The development of regulatory frameworks in India is an ongoing process, with efforts directed towards incorporating improved options for risk assessment and defining coverage. There is a discernible trend towards enhancing consumer protection and increasing transparency concerning the scope and limitations of cyber insurance policies (Wrede *et al*., 2020) [39].

6. **Economic and Managerial Implications**: Effective management of cyber incidents and comprehension of their economic implications are essential, as cyber insurance functions not only as a mechanism for financial risk transfer but also influences the operational behaviour of organizations managing cyber risks (Arce *et al*., 2024) [4].

12.2 Role of the Regulator (IRDAI)

1. **Introduction to the Indian Cyber Insurance Market:** The Indian cyber insurance market is an emerging sector dedicated to addressing the risks associated with cyber threats. Although it is a subset of the broader insurance industry, it is characterized by unique attributes owing to the inherently dynamic and complex nature of cyber risks.
2. **Role of the Insurance Regulatory and Development Authority of India (IRDAI):** The Insurance Regulatory and Development Authority of India (IRDAI) is instrumental in regulating the Indian insurance sector, including the area of cyber insurance. Its duties involve setting regulatory standards, ensuring market stability, and promoting the growth and development of the insurance sector.
3. **Regulatory Framework:** The IRDAI establishes a regulatory framework for cyber insurance by implementing guidelines and policies that govern the issuance, management, and claims processes of cyber insurance policies. This framework ensures that insurers maintain adequate capital reserves to address potential claims, as highlighted by the underestimation of risks in existing models such as Solvency II and the U.S. Risk-Based Capital standards (Eling & Schnell, 2019) [11].
4. **Addressing Challenges in Cyber Insurance:** The IRDAI is tasked with addressing significant challenges within the cyber insurance sector, including the lack of standardized frameworks, insufficient data for premium calculation, and the need for continuous feedback between insurers and policyholders (Lepoint *et al*. 2018) [22]. These challenges necessitate the development of innovative solutions and collaborations between the public and private sectors to enhance market functionality.
5. **Promoting Public-Private Partnerships:** The regulatory body plays a crucial role in fostering public-private partnerships to enhance cybersecurity measures and insurance coverage. This collaborative approach is beneficial for both insurers and policymakers (Woods & Simpson, 2017) [38].
6. **Regulatory Challenges and Market Evolution:** The evolving nature of cyber threats necessitates that the IRDAI continually update its regulatory frameworks to ensure their continued relevance and effectiveness. This process requires adaptation to technological advancements, such as blockchain technology, to improve transparency and automate processes (Farao *et al*., 2023) [13]. Furthermore, the IRDAI must address the regulatory risks and uncertainties that impact strategic decision-making within the industry, which may subsequently influence investment behaviour (Kianpour & Raza, 2024) [18].

The Insurance Regulatory and Development Authority of India (IRDAI) plays an important role in the Indian cyber insurance market. It creates rules to handle the specific problems of cyber risks. As the market changes, the IRDAI's actions will help keep the market stable, improve risk management, and support the growth of cyber insurance.

12.3 Interplay with Data Privacy Law

This document provides a comprehensive analysis of the development of the Indian Cyber Insurance Market, its regulatory framework, and its interaction with data privacy legislation.

1. **Evolution of the Indian Cyber Insurance Market:** The Indian cyber insurance market has experienced significant expansion, driven by the escalation of cyber threats and the need for effective risk management strategies. This expansion is partially attributed to technological advancements, which have resulted in the proliferation of data, thereby increasing susceptibility to cyber threats (Lepoint *et al*., 2018) [22]. The market faces challenges such as the absence of standardized frameworks for assessing cyber risks, insufficient data for premium calculations, and the diverse security postures of insured entities. These challenges necessitate an ongoing feedback loop between insurers and their clients to effectively manage risks (Lepoint *et al*., 2018) [22].
2. **Regulatory Framework:** India’s cyber insurance regulatory framework is evolving alongside initiatives to enhance cybersecurity legislation. The Information Technology Act of 2000, along with its subsequent amendments, established the foundation for cybersecurity regulations (Chandra, 2024) [5]. The enactment of India's Digital Personal Data Protection Act in 2023 represents a pivotal advancement in the nation's endeavour to protect personal data and align with international standards. This legislation offers a data protection framework that impacts cyber insurance policies by underscoring the necessity of adhering to rigorous data privacy regulations (Chandra, 2024) [5].
3. **Interplay with Data Privacy Law:** Cyber insurance is integral to assisting organizations in adhering to privacy laws and managing risks associated with data breaches. Insurers function as "compliance managers," offering risk management services that facilitate business alignment with legal regulations (Talesh, 2018) [34]. Establishing consumer trust through robust data protection measures is essential. The implementation of comprehensive data privacy laws in India has bolstered consumer confidence by mandating clear data protection protocols, which indirectly encourage the adoption of cyber insurance as a risk-mitigation strategy (Prastyanti & Sharma, 2024) [28].
4. **Challenges and Opportunities:** One of the primary challenges confronting the Indian cyber insurance market is the accurate assessment of cyber risks and determination of premium pricing, given the evolving nature of cyber threats and the paucity of historical data (Romanosky *et al*., 2017) [31]. The development of innovative cyber insurance solutions through technologies such as blockchain could enhance transparency, mitigate fraud, and optimize processes such as identity verification and claims automation, thereby establishing a robust foundation for market expansion (Farao *et al*., 2023) [13].

In summary, the Indian cyber insurance market is rapidly evolving, bolstered by a comprehensive regulatory framework designed to enhance cybersecurity and data privacy. Although significant challenges persist, technological advancements and careful alignment with data protection laws present promising opportunities to strengthen cybersecurity resilience in India.

12.4 Market Growth Drivers

The Indian cyber insurance market is expanding, propelled by several critical factors.

1. **Increasing Cyber Threats:** The increasing complexity and frequency of cyberattacks have compelled businesses to implement more robust cybersecurity measures. In conjunction with these measures, cyber insurance serves as a strategy for managing residual risks and mitigating financial losses (Dambra *et al*., 2020).
2. **Regulatory Influence:** Governments and policy-making institutions are increasingly acknowledging the significance of insurance in enhancing cyber-security standards. They may implement frameworks that support the integration of cyber insurance into broader cybersecurity policies (Woods & Simpson, 2017) [38].
3. **Market Demand:** Increasing global costs associated with cybercrimes underscore the growing necessity for cyber insurance. This trend is further highlighted by rising average claim values, which emphasize the urgent need for improved information sources to effectively manage cyber risks (Cremer *et al*., 2022) [8].
4. **Technological Advancements:** The integration of technologies such as blockchain, smart contracts, and self-sovereign identity presents viable solutions to the prevailing challenges in the cyber insurance sector, notably in addressing fraudulent claims and enhancing customer authentication, thereby improving market credibility and operational efficiency (Farao *et al*., 2023) [13].
5. **Insurer's Competitive Edge:** Insurers possessing a comprehensive understanding and the capability to accurately price cyber risks secure a competitive advantage, thereby fostering participation and growth within the cyber insurance sector (Xie *et al*., 2020) [40].
6. **Stakeholder Collaboration:** Fostering enhanced collaboration among insurers, policymakers, and cybersecurity stakeholders can result in the establishment of standardized and reliable frameworks, thereby facilitating market growth and maturity (Cremer *et al*., 2024) [8].
7. **Innovative Market Solutions:** The development of automated, real-time systems for monitoring and processing cyber insurance transactions via blockchain technology enhances transparency and establishes a reliable feedback loop among all parties involved (Lepoint *et al*., 2018) [22].

13. Current Market Landscape

This section of the study is organized into five distinct subsections: Market Size and Growth Trends, Key Players in the Market, Product Analysis, Types of Cyber Insurance Policies, and Standard Coverage Features. Each of these subsections is discussed in detail in the following sections.

13.1 Market Size and Growth Trends: The cyber insurance market in India is in its early stages and is experiencing rapid development. As cyber threats escalate and digital activities proliferate, businesses increasingly acknowledge the necessity of cyber insurance to mitigate the financial risks associated with cyber incidents (Arce *et al*., 2024; Cremer *et al*., 2022) [4, 8]. The average cost of a cyber incident has risen significantly, with global insurance claims increasing from US$145,000 in 2019 to US$359,000 in 2020. This trend highlights the urgent need for robust cyber risk management through insurance policies (Cremer *et al*., 2022) [8]. The absence of standardized data and reporting mechanisms presents a challenge; however, it also offers an opportunity for growth as solutions are developed (Cremer *et al*., 2022) [8]. Regulatory models require adaptation to address the specific characteristics of cyber risks, indicating the potential for market expansion and evolution as frameworks become more sophisticated (Eling & Schnell, 2019) [12].

13.2 Key Players in the Market: The cyber insurance market encompasses a variety of stakeholders, including underwriters, actuaries, claims specialists, and cyber operations specialists, each of whom plays a crucial role in decision-making processes related to underwriting and claims (Nurse *et al*., 2020) [25]. Insurers with a competitive edge in understanding and pricing cyber risks, particularly those providing professional surplus insurance, are pivotal actors in this domain (Xie *et al*., 2020) [40]. Additionally, the market comprises a diverse array of service providers who deliver post-breach expertise, including legal, technical, and communication support (Arce *et al*., 2024) [4].

13.3 Product Analysis

This document provides a comprehensive analysis of the current market landscape for cyber insurance in India, with particular emphasis on product analysis, standard coverage, exclusions, and target segments.

1. **Standard Coverage:** Cyber insurance policies in India generally encompass various risks, including data breaches, network security failures, business interruptions, and liabilities related to privacy breaches. These policies are structured to mitigate both direct and indirect losses arising from cyber incidents, such as expenses related to data restoration, legal fees, and regulatory penalties (Cremer, Murphy, *et al*., 2024; Romanosky *et al*., 2017) [9].
2. **Exclusions:** Cyber insurance policies commonly exclude coverage for damages resulting from intentional acts by the insured, cyber events related to war or terrorism, and expenses associated with the ongoing enhancement of security. Additionally, these policies may exclude certain types of procedural inadequacies or cyberattacks that are considered preventable (Cremer, Fortmann, *et al*., 2024; Wolff, 2023) [9].
3. **Target Segments:** The primary target segments for cyber insurance in India are medium-to large-scale enterprises that are substantially exposed to cyber risks. This includes sectors such as finance, healthcare, retail, and IT services, which manage significant volumes of sensitive data and are consequently more vulnerable to cyberattacks. Additionally, there is increasing interest among small businesses as awareness of cyber risks continues to rise (Nurse *et al*., 2020) [25].

13.4 Types of Cyber Insurance Policies

The current landscape of the cyber insurance market in India can be categorized into distinct policy types, primarily comprising standalone cyber policies and silent cyber or add-on covers.

1. **Standalone Cyber Policies:** These policies are specifically formulated to address cyber risks, offering comprehensive protection against a broad spectrum of cyber threats. Standalone policies typically encompass costs associated with data breaches, ransomware attacks, business interruptions, and regulatory fines (Xie *et al*., 2020) [40]. The risk associated with standalone policies is generally elevated because of their specificity and extensive coverage, resulting in variable premium rates and underwriting criteria (Xie *et al*., 2020) [40].
2. **Silent Cyber and Add-on Covers:** Silent cyber coverage pertains to exposure to cyber risks that are implicitly included in traditional insurance policies without explicit specification. These policies are not specifically designed for cyber coverage but may encompass cyber losses under certain interpretations of conventional coverage terms (Xie *et al*., 2020) [40]. Conversely, add-on covers are explicit endorsements attached to existing policies, offering additional cyber-related protection by broadening the scope of standard insurance products, such as property or liability insurance. Insurers and businesses are increasingly cognizant of the ambiguities associated with silent cyber risks, prompting efforts to clarify and explicitly define these risks within policy wording to mitigate unexpected liabilities (Cremer *et al*., 2024) [9].

These policy types exemplify the dynamic nature of the cyber insurance market as it adapts to address escalating threats within digital environments.

13.5 Standard Coverage Features

The current market landscape of cyber insurance in India encompasses two primary categories of coverage: first-party costs and third-party liability coverage. The following are the key aspects of each category.

13.5.1 First-Party Costs

1. **Data Breach and Crisis Management**: This encompasses expenses associated with the management and mitigation of a data breach, including public relations initiatives aimed at restoring the company's reputation.
2. **Business Interruption Losses**: Cyber insurance generally provides coverage for lost income resulting from business interruptions caused by cyber incidents.
3. **Data Recovery and Restoration**: Expenditures associated with data recovery and system restoration following a cyber-incident are encompassed within first-party coverage.
4. **Cyber Extortion and Ransom**: The policy may encompass expenses related to negotiating and fulfilling ransom demands in the event of a ransomware attack.

13.5.2 Third-Party Liability

1. **Network Security Liability:** This coverage safeguards against claims made by third parties who incur losses due to deficiencies in the insured party's network security.
2. **Privacy Liability:** Provision of coverage for legal defence expenses and settlements or damages arising from litigation associated with privacy breaches while ensuring adherence to data protection regulations.
3. **Regulatory Penalties:** Certain insurance policies may provide coverage for fines and penalties resulting from regulatory investigations; however, this coverage is contingent on the legal framework of the specific jurisdiction.
4. **Media Liability:** Safeguarding against third-party claims related to defamation or intellectual property infringement arising from online content.

These features represent dynamic developments within India's insurance sector, designed to address the escalating cyber threat landscape by providing coverage for both direct incident-related expenses and subsequent liabilities (Nurse *et al*., 2020) [25].

14. Challenges and Impediments to the Adoption of Cyber Insurance in India

This section is organized into five subsections: Lack of Awareness and Understanding, Pricing and Underwriting Complexities, Policy Standardization and Exclusions, Dynamic Threat Landscape, and Correlated and Systemic Risks. Each of these subsections is discussed below:

1. **Lack of Awareness and Understanding:** Cyber insurance is a relatively novel concept in India, with many businesses remaining unaware of its advantages and applications in risk management. Consequently, the demand for such policies is limited because of a lack of understanding of how cyber insurance can facilitate economic risk transfer and support business recovery following cyber incidents (Nurse *et al*., 2020) [25].
2. **Pricing and Underwriting Complexities:** The intricacies associated with the pricing and underwriting of cyber insurance policies present considerable challenges. Insurers frequently encounter difficulties in quantifying cyber risks because of insufficient data and the evolving nature of cyber threats. The calculation of premiums and underwriting decisions is further complicated by the diversity of incidents and their impacts, rendering it challenging to accurately assess and price these risks (Nurse *et al*., 2020) [25].
3. **Policy Standardization and Exclusions:** The cyber insurance sector in India is characterized by a significant lack of standardization. Insurers offer diverse coverage and exclusions, leading to confusion among potential policyholders. This variability can result in insufficient policy coverage and complicate the claims process, thereby posing challenges for businesses in understanding the scope and extent of coverage (Cremer *et al*., 2024) [9].
4. **Dynamic Threat Landscape:** The rapidly evolving nature of cyber threats presents significant challenges to the cyber insurance sector. Insurers must continuously update their risk assessment models and adapt to emerging attack types, such as ransomware and phishing. This dynamic threat environment complicates the maintenance of effective and relevant insurance products that can adequately address current cyber risks (Gurjar 2025) [14].
5. **Correlated and Systemic Risks:** Cyber risks are

frequently correlated owing to the interconnected nature of systems and infrastructures across various organizations and sectors. A single cyber incident can precipitate extensive repercussions across multiple entities, complicating the prediction and management of potential loss. This systemic characteristic of cyber risks poses a considerable challenge for insurers, as a solitary event can lead to significant cumulative losses (Palsson *et al*., 2020) [27].

These challenges underscore the intricate and multifaceted nature of implementing cyber insurance in India.

15. Lack of Awareness and Understanding:

This section of the study analyses the primary challenges facing the cyber insurance sector in India.

1. **Lack of Awareness and Understanding:** The cyber insurance market in India is in its nascent stages, and there is limited comprehension of cyber risks among businesses. This deficiency in awareness poses challenges in educating potential policyholders about the necessity and advantages of cyber insurance coverage. Enhanced public awareness and improved data availability are crucial for promoting understanding and engagement with cyber insurance products (Cremer *et al*., 2022) [8].
2. **Underwriting and Pricing Difficulties:** Accurately evaluating cyber risks for underwriting purposes presents significant challenges owing to the inherently unpredictable nature of cyber threats. Insurers encounter difficulties in appropriately pricing their products because they frequently lack comprehensive and standardized data on cyber incidents and losses (Cremer, Fortmann, *et al*., 2024) [9].
3. **Non-Standardized Policies:** The cyber insurance market in India, similar to global markets, is characterized by a lack of standardized policy wording, resulting in inconsistencies in coverage and exclusions. This situation can lead to confusion among potential policyholders as they endeavour to comprehend the scope of the coverage (Cremer *et al*., 2024) [9].
4. **Dynamic and Systemic Nature of Cyber Risk:** Cyber threats are rapidly evolving, and the interconnected nature of technologies exacerbates the complexity and potential risks associated with cyber incidents. The systemic nature of cyber risks suggests that a single cyber event can simultaneously affect multiple policyholders, thereby complicating risk assessment and management for insurers (Camillo, 2017) [6].
5. **The "Moral Hazard" Problem:** There is a concern that the availability of insurance may lead to complacency among insured entities, thereby diminishing their efforts to enhance cybersecurity. The challenge lies in ensuring that policyholders uphold high standards of cybersecurity to mitigate potential risks, even when they are insured (Arce *et al*., 2024) [4].

16. Case Studies

This study examines two case studies: a ransomware attack on an Indian manufacturing SME and a data breach at an Indian FinTech startup. These cases are discussed in detail in the following sections.

16.1 Case Study 1: A Ransomware Attack on an Indian Manufacturing SME

- **Incident Overview:** An Indian small and medium-sized enterprise (SME) in the manufacturing sector encountered a ransomware attack that significantly disrupted its operations. The attack involved the encryption of critical production files, accompanied by a ransom demand to secure their release.
- **Financial Impact:** The ransomware attack exerted considerable financial pressure, impacting not only the immediate costs associated with the ransom but also resulting in operational downtime, revenue loss, and potential reputational harm. Organizations incur additional expenses related to data restoration and implementing enhanced security measures (Shaikh *et al*., 2024) [30].
- **Cyber Insurance Response:** The small and medium-sized enterprise (SME) maintained a cyber insurance policy that offered essential financial support. This policy encompasses expenses associated with ransom payments (up to the policy limits), data recovery, forensic investigations, and legal counsel, thereby alleviating the overall financial impact of cyberattacks. Furthermore, the insurance policy provided guidance to SME in crisis management and stakeholder communication (Taskin *et al*., 2025) [35].
- **Lessons Learned and Prevention:** This case study emphasizes the significance of conducting regular risk assessments and implementing robust cybersecurity practices, illustrating how small and medium-sized enterprises (SMEs) can incorporate insurance into a comprehensive risk management strategy. This highlights the necessity of continuous employee training, updating of cybersecurity policies, and adoption of preventive technical measures as essential steps for future protection (Van Haastrecht *et al*., 2021) [36].

16.2 Case Study 2: A Data Breach at an Indian FinTech Startup

- **Incident Overview:** A leading Indian FinTech startup experienced a data breach that compromised sensitive customer information. This breach was the result of a sophisticated cyberattack that exploited vulnerabilities within the company's digital infrastructure (Kamuangu 2024).
- **Third-Party Liability:** Data breaches can result in substantial consequences, including potential liabilities for customers whose data are compromised. The startup faced the risk of legal actions and claims from affected individuals and business partners seeking compensation for privacy violations.
- **Regulatory Fines:** After the incident, the startup faced regulatory scrutiny and penalties due to its failure to adequately safeguard customer data, in accordance with Indian data protection laws. This situation highlights the financial sector's susceptibility to both operational disruptions and regulatory interventions (Rabbani *et al*., 2024) [29].
- **Cyber Insurance Response:** The company’s cyber insurance policy was instrumental in covering litigation costs, regulatory fines, and crisis management expenses. Additionally, insurance facilitates the management of third-party claims by providing

financial support and legal guidance, thereby stabilizing a startup's financial position during challenging periods (Olaiya *et al*., 2024) [26].

- **Risk Management Enhancement:** This case underscores the pivotal importance of adhering to cybersecurity frameworks and regulations, demonstrating the necessity of comprehensive risk management strategies. These strategies should encompass regular security audits, technological advancements, and employee training to prevent future incidents (Mustapha *et al*., 2023) [24].

17. Future Trends

Future trends are presented in detail below.

1. **Product Innovation**: An emerging trend is the development of parametric insurance products specifically designed for small and medium-sized businesses (SMBs). These products are structured to provide predetermined payouts upon the activation of specific parameters, thereby potentially streamlining claims processing for policyholders.
2. **Increased M&A and Partnerships:** Collaborations and mergers between insurance companies and cybersecurity firms are anticipated to increase in the future. Such alliances would enable insurers to utilize advanced cybersecurity technologies and insights, thereby enhancing their capacity to underwrite policies and manage cyber risks effectively.
3. **Bundling with Security Software/Services:** The integration of cyber insurance with cybersecurity software and services is likely to become increasingly common in the future. This strategy not only enhances the value of the insurance product but also aids in risk mitigation for clients by equipping them with essential security tools and services as part of their insurance packages.
4. **Impact of AI on Threats and Underwriting:** Artificial intelligence (AI) is projected to fulfill a dual function. On the one hand, it has the potential to enhance capabilities for identifying and mitigating cyber threats through advanced analytics and pattern recognition. Conversely, AI may also be employed in the underwriting process, enabling insurers to assess risks more accurately and tailor insurance products to better meet individual needs.

While these trends provide a general perspective, conducting specific research on cyber insurance in India would yield more comprehensive insights into the subject.

18. Recommendations for Stakeholders

The following recommendations are proposed for stakeholders engaged in India's cyber insurance sector:

18.1 For Regulators (IRDAI)

1. **Establish Comprehensive Guidelines:** Formulate explicit and comprehensive guidelines for cyber insurance policies to ensure uniform coverage across the industry, thereby promoting standardized terms and conditions for enhanced comprehension by all stakeholders.
2. **Enhanced Risk Assessment Standards:** Enhanced risk assessment protocols for insurers to improve the precision in evaluating cyber threats, thereby ensuring that policies accurately reflect emerging risks.
3. **Promote Awareness and Education:** Enhance initiatives to increase awareness of the significance and advantages of cyber insurance among businesses and the general populace, thereby promoting its adoption and improving preparedness against cyber threats.
4. **Encourage Collaboration:** Encourage collaboration among insurance companies, cybersecurity specialists, and technology providers to strengthen cyber resilience and establish a comprehensive framework for incident response and recovery.
5. **Facilitate Data Sharing:** Facilitate the exchange of anonymized incident data among insurance companies and regulatory bodies to enhance the comprehension of cyber threats and refine risk assessment models.

18.2 For Insurers

1. **Develop Tailored Products:** Specialized insurance products should be tailored to address the distinct needs of various business sectors, thereby reflecting the specific cyber risks they encounter.
2. **Enhancing Underwriting Processes:** Advanced technologies and analytics can be utilized to enhance the precision of underwriting and customize premiums according to individual risk profiles.
3. **Invest in Cyber Expertise:** Enhance internal cybersecurity capabilities by employing experts or collaborating with cybersecurity firms to improve product offerings and conduct comprehensive risk assessments.
4. **Foster Trust and Transparency:** Facilitate transparent communication with policyholders concerning terms, coverage, and claims processes to foster trust and credibility in cyber insurance.
5. **Focus on Risk Mitigation:** Enhanced services, such as risk assessments and cyber hygiene training, should be provided to aid policyholders in reducing their exposure to cyber risks.

18.3 For Businesses

1. **Evaluate Cyber Insurance Needs:** Conduct comprehensive evaluations of your organization's exposure to cyber risks and incorporate cyber insurance as a fundamental component of your risk-management strategy.
2. **Implement Robust Cybersecurity Measures:** Investing in cybersecurity infrastructure and practices serves not only to reduce insurance premiums but also to enhance protection against potential threats.
3. **Engaging with Insurers:** Collaboratively engage with insurance providers to gain a thorough understanding of policy specifications and coverage, and actively engage in risk assessment procedures to ensure comprehensive insurance coverage.
4. **Regular Risk Assessments:** It is imperative to continuously monitor and evaluate cybersecurity protocols to adapt to evolving threat landscapes and ensure their alignment with insurance coverage requirements.
5. **Promoting Employee Awareness:** Implementing regular training and awareness programs for employees is essential to fortify the cybersecurity culture within an organization and mitigate the risk of cyber incidents attributable to human error.

19. Findings of the Study

The principal findings of this study concerning cyber insurance in India, as derived from the discussions provided, are as follows:

1. The cyber insurance market in India is growing rapidly. This is because more people are using digital technology and are facing cyber threats. However, challenges remain. There is no standard data; risk assessment is complex, and many people are unaware of it.
2. Businesses face significant challenges with cyber insurance. Many people do not know or understand its benefits. Pricing and underwriting are difficult because of insufficient data. Policies are not standardized, causing confusion. Cyber threats change quickly, and cyber risks are often linked and widespread.
3. The insurance rules are changing significantly. The Insurance Regulatory and Development Authority of India (IRDAI) is important for setting these rules. New laws, such as the Digital Personal Data Protection Act 2023, are affecting cyber insurance policies.
4. Market growth is driven by more cyber threats and attacks, rules that encourage buying cyber insurance, higher costs from cybercrime, new technology such as blockchain, and teamwork among insurers, policymakers, and cybersecurity experts.
5. Standard coverage usually includes costs for the company itself, such as handling a data breach and loss of business. It also covers costs for others, such as privacy issues and fines from regulators.
6. Case studies show how cyber insurance helps small and medium-sized businesses and startups recover from ransomware attacks and data breaches.
7. Future changes will include new products, better teamwork between insurance companies and cybersecurity firms, the combination of insurance with security services, and the use of artificial intelligence in the insurance process.
8. It is suggested that clear rules be created, risk assessment be improved, awareness be raised, information be shared, and special products be developed for different areas.

20. Conclusion

The cyber insurance market in India is experiencing rapid development; however, it faces significant challenges as it advances. Despite the increasing demand driven by heightened digitalization and cyber threats, several critical issues warrant attention. A major impediment to adoption is the lack of awareness and understanding among businesses of the benefits and coverage of cyber insurance. Pricing and underwriting complexities persist, primarily because of insufficient data and the dynamic nature of cyber risks. Non-standardized policies and ambiguous exclusions contribute to policyholder confusion. The rapidly changing threat landscape complicates insurers' efforts to maintain policy relevance and accurately assess risks. The correlated and systemic nature of cyber risks presents challenges for insurers in managing potential losses. To overcome these challenges and foster a robust cyber insurance market in India, a multi-stakeholder approach is required. Regulators, such as the Insurance Regulatory and Development Authority of India (IRDAI), should establish comprehensive guidelines, enhance risk assessment standards, promote awareness, and facilitate data sharing to this end. Insurers must develop tailored products, refine underwriting processes, invest in cyber expertise, and focus on risk-mitigation services. Businesses should evaluate their cyber insurance needs, implement robust cybersecurity measures, proactively engage with insurers, and promote employee awareness. As the digital economy expands, cyber insurance will play an increasingly critical role in India's risk management landscape. Addressing the current limitations through collaborative efforts among regulators, insurers, and businesses can foster a more resilient cyber insurance ecosystem. Continued research and innovation are essential to keep pace with evolving cyber threats and provide effective risk transfer mechanisms for Indian organizations.

References

1. Adarsh, Patil M. Cyber liability insurance: the future of Indian e-commerce infrastructure. Bharati Law Review. 2017; p.12-20.
2. Adriko R, Nurse JRC. Does cyber insurance promote cyber security best practice? An analysis based on insurance application forms. Digital Threats: Research and Practice. 2024;5(3):25. doi:10.1145/3676283
3. Anu P. Cyber insurance. Int J Res Publication Rev. 2023;4(3):4586-4589.
4. Arce D, Woods DW, Böhme R. Economics of incident response panels in cyber insurance. Comput Secur. 2024;140:103742. doi:10.1016/j.cose.2024.103742
5. Chandra AC. Strengthening India's cybersecurity and data privacy landscape: a comprehensive overview. Indian J Public Adm. 2024;70(3):466-478. doi:10.1177/00195561241271616
6. Camillo M. Cyber risk and the changing role of insurance. J Cyber Policy. 2017;2(1):53-63. doi:10.1080/23738871.2017.1296878
7. Cremer F, Fortmann M, Ryan BJ, Materne S, Mullins M, Sheehan B. On the insurability of cyber warfare: an investigation into the German cyber insurance market. Comput Secur. 2024;142:103886. doi:10.1016/j.cose.2024.103886
8. Cremer F, Murphy F, Mullins M, Sheehan B, Kia AN, Fortmann M, *et al*. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 2022;47(3):698-736. doi:10.1057/s41288-022-00266-6
9. Cremer F, Murphy F, Sheehan B, Materne S, Mullins M, Fortmann M. Bridging the cyber protection gap: an investigation into the efficacy of the German cyber insurance market. Risk Manag Insur Rev. 2024;27(1):57-87. doi:10.1111/rmir.12261
10. Dambra S, Bilge L, Balzarotti D. SoK: cyber insurance - technical challenges and a system security roadmap. IEEE Symp Security Privacy. 2020;3:1367-1383. doi:10.1109/sp40000.2020.00019
11. Eling M, Schnell W. What do we know about cyber risk and cyber risk insurance? J Risk Finance. 2016;17(5):474-491. doi:10.1108/jrf-09-2016-0122
12. Eling M, Schnell W. Capital requirements for cyber risk and cyber risk insurance: an analysis of Solvency II, the U.S. risk-based capital standards, and the Swiss solvency test. North Am Actuar J. 2019;24(3):370-392. doi:10.1080/10920277.2019.1641416
13. Farao A, Paparis G, Panda S, Panaousis E, Zarras A, Xenakis C. INCHAIN: a cyber insurance architecture

with smart contracts and self-sovereign identity on top of blockchain. Int J Inf Secur. 2023;23(1):347-371. doi:10.1007/s10207-023-00741-8
14. Gurjar S. Cybersecurity in cloud-based insurance: a comprehensive analysis of risks and solutions. World J Adv Res Rev. 2025;26(1):2610-2619. doi:10.30574/wjarr.2025.26.1.1320
15. Kamuangu P. A review on cybersecurity in fintech: threats, solutions, and future trends. J Econ Finance Account Stud. 2024;6(1):47-53. doi:10.32996/jefas.2024.6.1.5
16. Katiyar DN, Sahu DAK, Kumar MP, Verma MS, Saxena DS, Tripathi MS. AI and cyber-security: enhancing threat detection and response with machine learning. Educ Admin Theory Pract. 2024;30(4). doi:10.53555/kuey.v30i4.2377
17. Khalili MM, Liu M, Naghizadeh P. Designing cyber insurance policies: the role of pre-screening and security interdependence. IEEE Trans Inf Forensics Secur. 2018;13(9):2226-2239. doi:10.1109/tifs.2018.2812205
18. Kianpour M, Raza S. More than malware: unmasking the hidden risk of cybersecurity regulations. Int Cybersecur Law Rev. 2024;5(1):169-212. doi:10.1365/s43439-024-00111-7
19. Kumar J, Mukhopadhyay S, Puri P. Cyber risk insurance - an Indian perspective. Int J Adv Res. 2016;4(7):1-10.
20. Kumar R, Singh S. Cyber insurance in India: an overview. Int J Res Finance Manag. 2023;6(1):373-378. doi:10.33545/26175754.2023.v6.i1d.230
21. Lau P, Ten C-W, Liu Z, Wang L, Wei W. A coalitional cyber-insurance design considering power system reliability and cyber vulnerability. IEEE Trans Power Syst. 2021;36(6):5512-5524. doi:10.1109/tpwrs.2021.3078730
22. Lepoint T, Eldefrawy K, Ciocarlie G. Block CIS—A blockchain-based cyber insurance system. IEEE IC2E. 2018;52:378-384. doi:10.1109/ic2e.2018.00072
23. Marotta A, Martinelli F, Nanni S, Orlando A, Yautsiukhin A. Cyber-insurance survey. Comput Sci Rev. 2017;24:35-61. doi:10.1016/j.cosrev.2017.01.001
24. Mustapha I, Binti Yusof SH, Jahanzeb A, Vaicondam Y, Usmanovich B. Cybersecurity challenges and solutions in the fintech mobile app ecosystem. Int J Interact Mob Technol. 2023;17(22):100-116. doi:10.3991/ijim.v17i22.45261
25. Nurse JRC, Creese S, Goldsmith M, Agrafiotis I, Axon L, Erola A. The data that drives cyber insurance: a study into the underwriting and claims processes. IEEE CyberSA. 2020;5:1-8. doi:10.1109/cybersa49311.2020.9139703
26. Olaiya O, Ajayi O, Adesoga T, Adebayo Y, Olagunju O, Ojo A. Cybersecurity strategies in fintech: safeguarding financial data and assets. GSC Adv Res Rev. 2024;20(1):50-56. doi:10.30574/gscarr.2024.20.1.0241
27. Palsson K, Shetty S, Gudmundsson S. Analysis of the impact of cyber events for cyber insurance. Geneva Pap Risk Insur Issues Pract. 2020;45(4):564-579. doi:10.1057/s41288-020-00171-w
28. Prastyanti RA, Sharma R. Establishing consumer trust through data protection law as a competitive advantage in Indonesia and India. J Hum Rights Cult Legal Syst. 2024;4(2):354-390. doi:10.53955/jhcls.v4i2.200
29. Rabbani H, Shahid MF, Khanzada TJS, Siddiqui S, Jamjoom MM, Ashari RB, *et al*. Enhancing security in financial transactions: a novel blockchain-based federated learning framework for detecting counterfeit data in fintech. PeerJ Comput Sci. 2024;10:e2280. doi:10.7717/peerj-cs.2280
30. Rehman Shaikh MU, Savita KS, Mandala S, Ullah R, Akbar R. Fortifying against ransomware: navigating cybersecurity risk management with a focus on ransomware insurance strategies. Int J Acad Res Bus Soc Sci. 2024;14(1). doi:10.6007/ijarbss/v14-i1/20566
31. Romanosky S, Ablon L, Kuehn A, Jones T. Content analysis of cyber insurance policies: how do carriers write policies and price cyber risk? RAND Corporation. 2017. doi:10.7249/wr1208
32. Routaray S, Arya M, Agnihotri R. Cyber insurance need of the hour: to combat growing cyber-attacks within cyber space. Libr Prog Int. 2024;44(3):12748-12754.
33. Singh A. Impacts of technological advances on insurance sector: a study on cyber insurance in India. Indian J Integr Res Law. 2024;4(3):894-915.
34. Talesh SA. Data breach, privacy, and cyber insurance: how insurance companies act as "compliance managers" for businesses. Law Soc Inq. 2018;43(2):417-440. doi:10.1111/lsi.12303
35. Taskin N, Ercan HD, Özkeleş Yıldırım A, Metin B, Wynn M. Cyber insurance adoption and digitalisation in small and medium-sized enterprises. Information. 2025;16(1):66. doi:10.3390/info16010066
36. Van Haastrecht M, Spruit M, Baumgartner L, Mallouli W, Shojaifar A, Sarhan I. A threat-based cybersecurity risk assessment approach addressing SME needs. ACM Int Conf. 2021;1-12. doi:10.1145/3465481.3469199
37. Wolff J. The role of insurers in shaping international cyber-security norms about cyber-war. Contemp Secur Policy. 2023;45(1):141-170. doi:10.1080/13523260.2023.2279033
38. Woods D, Simpson A. Policy measures and cyber insurance: a framework. J Cyber Policy. 2017;2(2):209-226. doi:10.1080/23738871.2017.1360927
39. Wrede D, Graf Von Der Schulenburg J-M, Stegen T. Affirmative and silent cyber coverage in traditional insurance policies: qualitative content analysis of selected insurance products from the German insurance market. Geneva Pap Risk Insur Issues Pract. 2020;45(4):657-689. doi:10.1057/s41288-020-00183-6
40. Xie X, Eling M, Lee C. Cyber insurance offering and performance: an analysis of the U.S. cyber insurance market. Geneva Pap Risk Insur Issues Pract. 2020;45(4):690-736. doi:10.1057/s41288-020-00176-5
41. Zhang R, Hayel Y, Zhu Q. A bi-level game approach to attack-aware cyber insurance of computer networks. IEEE J Sel Areas Commun. 2017;35(3):779-794. doi:10.1109/jsac.2017.2672378