Page 2476 - 2487

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Cyber Insurance in India: Legal Framework, Gaps, and Risk Mitigation

NEHA GUPTA[1] AND DR. PIYUSH KUMAR TRIVEDI[2]

ABSTRACT

With the growing importance of cyber insurance being recognized in India, there are increasing instances of companies opting for it in light of rising cyber threats. Such recognition is highlighted in the startling finding of CERT-In where over 2.04 million cybersecurity cases were observed during the year 2024 . Therefore, it becomes essential to understand the current state of the cyber insurance market through the legal and regulatory framework prevailing in India, particularly given the existence of the Digital Personal Data Protection (DPDP) Act, 2023.

The analysis of these dynamics brings forth various gaps that require further discussion, particularly the very low market penetration rate of less than 1%, the problem of high premiums, exclusions in policies, and the overall lack of awareness surrounding the topic. There are multiple ways through which these gaps may be addressed.

As a result of analyzing the characteristics of products, gaining insights from case studies, and monitoring market trends, the intrinsic value of cyber insurance can be identified. While simply an instrument to transfer risk financially, cyber insurance is an important aspect of incident response and a motivating factor in advocating for improved cybersecurity. In this context, suggestions for standardizing policies, incentivizing the uptake through regulatory measures, and encouraging private-public cooperation have been proposed as vital approaches that could help promote cyber insurance as a valuable tool.

Keywords: *Cyber insurance, IRDAI, DPDP Act 2023, cyber risks, business mitigation, India*

I. INTRODUCTION

The digital economy of India has witnessed an impressive growth trend, packed with numerous opportunities but also fraught with mounting risks from cyber attacks. It has always been the National Crime Records Bureau that has kept close watch on the rising incidence of cybercrimes and provided insights into the prevailing problems. The Data Security Council of India and CERT-In have issued warnings against imminent threats to enterprises posed by ransomware attacks, data leaks, and phishing schemes. Recent trends have indicated a growing cost burden

[1] Author is an LL.M. Student at Khwaja Moinuddin Chishti Language University, Lucknow, India.
[2] Author is an Associate Professor at Khwaja Moinuddin Chishti Language University, Lucknow, India.

 [ISSN 2581-5369]

related to data breaches in other parts of the world.

Significantly, the occurrence of cyber risks within particular sectors such as insurance is indicative of the weaknesses that exist in the digital environment. Against the backdrop of rising threats, cyber insurance has emerged as an indispensable tool for the management of these risks through the transfer of any liabilities incurred during cyber attacks onto the insurance companies. The scope of this insurance includes both direct costs such as the payment of ransoms and forensics as well as indirect costs including fines for non-compliance with regulations and legal fees. In spite of the predicted rapid growth rate of the cyber insurance industry, which will see its value rise from USD 0.58 billion in 2025 to USD 5.64 billion in 2034 with a CAGR of 28.76%,[3] actual uptake remains low, emphasizing the existence of gaps in ensuring protection against these risks. Against this background, this analysis provides insights into cyber insurance with a focus on the gaps that exist and the importance of mitigation measures in April 2026.

II. LEGAL AND REGULATORY FRAMEWORK

Cyber insurance in India operates under general insurance laws, with no standalone statute. Key elements include:

- **IRDAI's Oversight:** IRDAI is one of the major entities that play an important role in regulating the regulations pertaining to insurance products. It regulates the product designing, approval, and distribution processes to protect the interest of consumers as well as market stability. During the fiscal year 2018–19, IRDAI came out with a standardized Cyber Security Insurance Policy template having a unique identification number as IRDAN106P0001V01201819. [4]The said template acts as a basic framework for designing cyber insurance products under regulatory norms.

Irrespective of the changes made in the template, insurance companies need the permission of IRDAI before issuing the policy as per the modified version. Furthermore, keeping in view the changing dynamics of risks associated with the internet and the growing relevance of cybersecurity, IRDAI issued a note in 2020 via a working group in order to facilitate cyber insurance products as well as enhance its coverage through add-ons.

[3] The Report Cubes, India Cyber Insurance Market Growth, Scope & Outlook 2034 (projecting growth from USD 0.58 billion in 2025 to USD 5.64 billion by 2034 at a CAGR of 28.76%).
[4] Insurance Regulatory and Development Authority of India (IRDAI), Cyber Security Insurance Policy Template, UIN: IRDAN106P0001V01201819 (issued 2018–19).

 [ISSN 2581-5369]

By stimulating innovations and ensuring the provision of specific types of insurance products which help in mitigating particular risks, for instance, cyber threats, the IRDAI seeks to strengthen the capacity of the insurance industry to guard people against any form of financial risks. The regulations provided by the IRDAI not only provide protection to the interest of the policy holders, but also ensure that insurance companies keep on evolving by providing the best insurance solutions based on their clients' demands.

Key Policy Features (from IRDAI Template):

- **Insuring Clauses**: The insurance policy offers extensive protection from financial loss due to several forms of "Cyber Event" such as hacking, theft, or other incidents involving the use of computers. The incidents must be identified and reported in the policy period in order to trigger the coverage.

One part of this protection package includes the obligation to take actions within 72 hours of the occurrence of the cyber event. This means undertaking numerous actions such as handling the event through forensic examination, PR campaigns, and legal advice.

In addition to these costs, the insurance policy also covers notification expenses as well as monitoring expenses to make sure that no additional damages occur. Restoration and business interruption costs can also be covered.

In addition to this, the insurance also provides for the inclusion of any additional expenses incurred by the business for addressing the effects caused by the cyber attack, including the implementation of more stringent cybersecurity practices to avoid similar events in the future. In addition, such insurance may even cover regulatory fines and penalties if they are covered by the insurance policy.

Thus, such insurance serves as an umbrella of safety for organizations that are increasingly threatened by cyber attacks.

First-Party vs. Third-Party: Comprehensive first-party recovery and third-party liability.

Extensions: The new subsidiaries will be integrated into the company's system automatically, thus simplifying this step. Also, there are options for additional coverages, which include contingent business interruption insurance, network fraud insurance, goodwill towards customers, and PCI-DSS compliance problem-solving. Optional coverage provides businesses with a range of opportunities to customize their insurance policy in the best way to cope with possible dangers and threats efficiently. By creating these options, the company seeks to increase the efficiency of its services by providing businesses with numerous possibilities to

 [ISSN 2581-5369]

use the benefits offered by the organization to their fullest extent and thus cope with potential problems successfully. The inclusion of such an option into the service offered by the company can be considered another reflection of the business' commitment to addressing all types of risks that could arise. Thus, the company demonstrates its willingness to provide businesses with a wide range of tools that would enable them to cope with their problems and challenges efficiently.

- **Obligations:** In addition, the insured party should adopt and diligently maintain the adequate level of security measures to ensure proper protection of the assets. In case any security incident occurs, it will be necessary to notify the company about the occurrence of the incident via the designated hotline number so that an effective course of action may be taken promptly by the Incident Coordinator. Moreover, the insured party is also required to cooperate with the company in the process of mitigation of the security incident. This may include providing necessary data to help investigate the matter and adopting strategies suggested by the Incident Coordinator to mitigate the security incident. It can thus be seen that the insured party plays an important role in asset protection through the implementation and maintenance of reasonable security measures and prompt cooperation in mitigation activities.

- **Exclusions:** The known matters are numerous and include but are not limited to events, happenings, scientific discoveries, social matters that attract the attention and interest of individuals across the world. Acts of intention can be viewed as conscious and deliberate actions taken by individuals, groups or organizations with certain intentions in view. The effects of wars and terrorism, other than cyber terrorism, go beyond destruction as they affect several aspects of the economy and individual people. Lack of appropriate security exposes the concerned parties to various risks. It is therefore important that proper security measures be put in place. Betterment involves efforts and actions that aim at improving one's self and situation or making progress in any area of life.

Interplay with Other Laws:

- **IT Act, 2000 (Section 43A, 72A)** and **CERT-In Directions**:

The reporting of incidents should be made mandatory in order to strengthen cybersecurity efforts. The reason being that it will allow for security breaches or any security incidents to be identified and recorded in order to mitigate potential problems that might result due to any breach or security threats. Not only will incident reporting assist in improving cybersecurity in general, but it will also facilitate effective incident management.

 [ISSN 2581-5369]

In addition to the above, in terms of cybersecurity risk mitigation efforts, the provision of cyber insurance can play a significant role in helping mitigate risks related to cybersecurity. In order to prevent any type of risk in terms of data breaches or compliance costs, organizations take up cyber insurance that can cover their losses in case something happens to them due to such issues.

- **DPDP Act, 2023 & Rules 2025:**

Prompt notification of the Data Protection Board under the duty to act without delay should be given in instances where there is a data breach. The 72-hour period serves as a significant time window within which the organization should report to avoid breaching any law.[5] Moreover, notifying the individual affected is another key step in ensuring that the organization remains compliant. The compliance with these timelines increases the probability of liabilities that the organization is likely to incur. To reduce the impact of the penalties, fines, and defense fees associated with this process, cyber insurance coverage becomes necessary. The benefits of obtaining cyber insurance coverage include mitigating the costs associated with notifications, fines, and legal costs incurred due to the breach. Compliance with these requirements ensures that the organization remains within the boundaries of the law. Furthermore, it assists the company in defending itself from legal action taken on account of its failure to notify the concerned parties regarding a breach.

- **IRDAI's Sector-Specific Guidelines:**

The 2026 Information and Cyber Security Guidelines, issued in April 2026, are expected to include alignment with the Data Protection and Data Privacy (DPDP) regulations, the relevance of board-level governance, risk review quarterly, improvement in control mechanisms related to outsourcing and cloud computing, incident reporting requirements, and requirement of regular audit for insurers and intermediaries. The focus of these guidelines being on insurers' ability to maintain their resiliency, indirectly results in improving their product availability and pricing stability. In addition, the 2025 Insurance Fraud Monitoring Framework is designed to be put into practice in 2026 and is aimed at preventing the incidence of cyber fraud. It demonstrates that the insurance industry does not remain indifferent towards emerging cyber security threats and is willing to adopt measures necessary to counter them and protect the industry from possible harm caused by fraudsters. Further, through fostering a culture of transparency and accountability, such programs contribute significantly towards boosting the confidence of stakeholders and enhancing the ability of the sector to cope with cyber threats.

[5] Digital Personal Data Protection Act, 2023, § 8 (India); Digital Personal Data Protection Rules, 2025, Rule 7(2) (requiring notification to the Data Protection Board within 72 hours of becoming aware of a personal data breach).

 [ISSN 2581-5369]

On balance, it is clear that the above comprehensive measures illustrate the significance of implementing appropriate cybersecurity programs within the insurance sector.

- **Sectoral Nuances**: RBI and SEBI impose additional requirements for banking/financial services.

III. GAPS AND CHALLENGES

Despite the framework, several gaps persist:

- **Low Penetration and Awareness**:

Only less than 1% of companies in India have insurance at present. This low percentage is much lesser than over 30% of the coverage rates in the United States. This significant difference reflects the existence of considerable disparities in the insurance rates for SMEs in these two countries. The first cause of such gaps between SMEs' coverage rates could be linked to the idea that SMEs consider insurance rates too high for themselves to afford them. In addition, another reason for this situation might be associated with the misconception of the coverage level held by many SMEs. As a result, most Indian businesses do not have any insurance and thus face many threats to their well-being. Therefore, it is crucially important for the insurance sector to work on solving the problem of affordability of insurance services by offering affordable and flexible policies to meet the needs of SMEs. By doing this, it will be possible to promote a higher level of SME coverage within the country.

- **Underwriting and Pricing Issues:**

Due to the limitation of insufficient claims data in history, insurance firms are obliged to impose high premiums and follow an ultra-conservative approach in underwriting. This is because of the risk and uncertainties that are inherent in the absence of sufficient data in predicting and evaluating possible losses. Nevertheless, in the ever-changing cybersecurity environment, there is an issue in conventional models and practices as they are unable to cope with the fast-evolving cybersecurity risks, including those involving artificial intelligence-based threats and ransomware, which are developing faster than the present risk evaluation frameworks can handle. This has led to an increased demand for insurance companies to rethink their underwriting processes and become more adaptive in order to successfully counter these new risks. With the help of innovation and the use of technological advancements, insurance firms can improve their capacity to respond to changes in the cyber risk environment and offer more extensive protection for their clients. In such a setting, being ahead of the game necessitates a forward-looking approach to risk management and an ongoing effort to upgrade their

 [ISSN 2581-5369]

underwriting process to deal with emerging cyber risks.

- **Policy Gaps and Exclusions:**

Many elements result in high denial rates when it comes to insurance, which can be up to 62% according to some surveys. The most common reasons why an insurance policy does not cover losses include ambiguous language, exclusion of coverage in the case of war and terroristic activities, and limited scopes of coverage. As a result, the insured parties might find themselves in trouble because their claims will be refused despite the fact that insurance should provide certain protection. It is also noteworthy that insurance policies do not cover systemic risks or acts sponsored by other states, which makes matters even more complicated for the insured parties who want to be compensated for the losses incurred. Considering the constantly growing complexity and dynamic nature of risks in the current reality, it is imperative for insurance companies to solve such problems and offer people better options for their policies.

- **Regulatory and Standardization Deficits:**

Unlike some other nations where there is a requirement to purchase cyber insurance as part of regulatory compliance, in India, there is no mandate to buy the insurance cover. This is one reason why the policies available from various insurers in India vary greatly. It should be mentioned that the template for cyber insurance created by the Insurance Regulatory and Development Authority of India (IRDAI) in 2018 is yet to undergo significant revisions in accordance with the upcoming DPDP law or cyber threats predicted by 2026. In spite of the fact that there is no obligation to purchase cyber insurance in India at the moment, people are still strongly advised to take into consideration the necessity of buying such insurance due to possible dangers that can arise because of cyber security problems. One of the important things that need to be considered in connection with the topic is the ongoing cyber threats development which requires being kept track of by those interested in cyber insurance. Therefore, it is necessary to monitor all changes related to cyber insurance products in order to provide maximum security.

- **Claims and Enforcement:**

The complexities associated with proofing the occurrence of a Cyber Event pose challenges in processing insurance claims owing to moral hazard as well as lack of standardized databases. In sum, the two issues make it difficult to handle claims effectively within the insurance industry. For instance, recent cases of cyber security threats include Star Health where about 31

 [ISSN 2581-5369]

million customers were affected.[6] Such vulnerabilities do not only affect insurance companies but also other players in the industry. Thus, there is much difficulty in dealing with claims relating to cyber events. Moral hazard is another challenge faced by insurance firms when dealing with cyber events because such cases make it hard to process claims. The lack of standardized database makes it even difficult for insurance firms to process claims relating to cyber events. It is worth noting that the database could have been used to ascertain the magnitude of the damage done by the cyber attack. The case of Star Health has made it clear how vulnerable insurance firms are to threats in cyber space. The insurer was affected by a breach in the system and therefore, had to handle complaints from many clients.

- **SME-Specific Barriers:**

The prohibitive cost that must be met when introducing advanced cybersecurity practices into a business organization, coupled with a possible lack of in-house cybersecurity skills, acts as strong impediments to the uptake of such practices. Other than the financial considerations and the potential lack of skilled personnel within an organization, another factor that makes it difficult for a company to adopt advanced cybersecurity practices is the belief that cybersecurity may not be pertinent to its operations or the particular industry in which it operates. Overall, therefore, a number of obstacles face business organizations in the pursuit of improved cybersecurity practices; indeed, the cost, skill level, and even the idea of how pertinent cybersecurity might be can all work as major deterrents towards the effective incorporation of cybersecurity policies in an organization. To overcome these obstacles and introduce effective cybersecurity practices into a business organization, the firm needs to be deliberate in making efforts to incorporate cybersecurity technology and skills, while also ensuring that the firm recognizes the relevance of such measures to its business activities.

IV. ROLE IN MITIGATING CYBER RISKS FOR BUSINESSES

Cyber insurance goes beyond indemnity to act as a proactive risk management tool:

- **Financial Risk Transfer**:

Coverage of cybersecurity incidents under the insurance policy covers a broad array of aspects. It includes compensation for any direct loss incurred due to ransomware attacks or expenses required to restore the stolen data. The insurance also provides cover for all sorts of indirect expenses incurred due to such incidents. Indirect expenses include loss of business, which is

[6] See Reuters, Star Health Hacker Says Death Threats and Bullets Sent to Executives (May 9, 2025) (reporting breach affecting over 31 million customers); India Today, Star Health Acknowledges Data Breach Affecting 31 Million Customers (Oct. 10, 2024).

 [ISSN 2581-5369]

compensated for by business interruption insurance. Other indirect expenses include legal costs that might accrue as a result of cybersecurity incidents; these costs are compensated for by special insurance policies. Public relations expenses incurred in response to cybersecurity incidents can also be compensated for under the insurance policies. Such a combination of insurance coverages makes sure that businesses affected by cybersecurity incidents recover rapidly from their effects. As a consequence, companies will be able to overcome cyber incidents without suffering any financial blow that might affect their financial status.

- **Incident Response Support:**

According to corporate policy, it is important to ensure access to Incident Coordinators who will be responsible for managing and controlling incidents, as well as other professionals who have pre-approved qualifications to address different kinds of security threats. At the same time, it is necessary to have insurance regarding forensics and notification procedures since they are critical in order to comply with all deadlines stipulated by the DPDP requirements. These policies not only highlight fast and effective measures in dealing with security incidents, but they also stress the importance of being prepared and having adequate means to tackle any situation related to security threats. Overall, it is evident that these policies are critical for ensuring an organized approach to dealing with security incidents.

- **Incentivizing Best Practices:**

For starters, underwriters require that the implementation of appropriate cybersecurity controls, such as multi-factor authentication and regular data backups, be mandatory in order to qualify for reduced insurance rates or even be insured in the first place. The reason why underwriters require this control is to ensure that the organization is well-positioned to protect itself from any possible cyber threats. Lastly, the post-incident "Revamp Advice Costs" become relevant to the conversation when it comes to organizations receiving financial help from a third party, namely, the insurance company, after experiencing a cyber incident in order to make sure that the company undergoes an effective process of remediation and recovery. Essentially, this financial resource will assist the firm in strengthening its security systems and making adjustments so that future incidents are prevented. Thus, the concept of underwriters requiring certain cybersecurity controls can be viewed in several ways. First, there is the possibility of reducing the insurance rate. Second, underwriters provide advice regarding how the organization can recover from a recent cyber attack. Third, underwriters help the company become more resilient in terms of cybersecurity.

 [ISSN 2581-5369]

- **Business Continuity:**

Extensions in Building Information (BI) like integration of an automatic monitoring system as well as installation of cybersecurity tools are some of the useful approaches that would go a long way in reducing any operational downtime. This is because through the utilization of such approaches, companies will be in a good position to safeguard themselves from various attacks and hence ensure smooth running of business operations.

The availability of resources that help in tackling downtime will enable SMEs and start-up firms to perform effectively in competition with large firms. It is because in doing so, they will prevent disruptions of operations while at the same time ensuring that they can compete favorably with bigger firms in the market. In modern times, in which businesses rely heavily on technology to propel their growth, the need to reduce downtime with the help of BI extensions and effective measures to mitigate risks becomes an integral aspect that helps them gain a competitive advantage. The companies that opt to implement such initiatives show how committed they are to being reliable and resilient, which might be valuable for their image in the eyes of their customers and other stakeholders.

Through the use of BI extensions and mitigation costs, SMEs and startups prove their readiness to strive for excellence and to explore new solutions to achieve sustainable growth. Such actions protect them from potential threats while positioning them as companies that can successfully compete even in the dynamic business environment.

Case Studies

In the Manufacturing SME Ransomware Attack scenario, the problem was the encryption of important documents. Luckily, the insurance policy worked in favor of the firm, which covered the ransom payment (within certain limits) and the costs for recovering the information, investigating the crime, conducting legal proceedings, and managing the crisis. These advantages allowed the business to quickly restore its activities and report the problem to relevant parties.

As for the FinTech Startup Data Breach, the problems were completely different. The leakage of client information led to liabilities and fines. Fortunately, there was an insurance policy that covered the costs of the litigation process, regulatory fines, and notification, which helped the firm recover from this problem.

An interesting development in the insurance market is the cooperation between insurance companies and cybersecurity firms. The cooperation seeks to offer bundled services where the knowledge and expertise of cybersecurity firms are combined with the insurance offered by

 [ISSN 2581-5369]

insurance companies. Another developing trend within the insurance sector is the application of artificial intelligence in the underwriting process and the introduction of parametric insurance products designed especially for small and medium enterprises.

V. Recommendations and Future Outlook

The predicted expansion of the market in the coming years indicates that cyber insurance will likely become an integral part of India's digital economy, provided that existing gaps are addressed properly. There are several reasons behind this prediction, such as continued work to standardize the RDAI templates and mitigate risks connected with AI/deepfake technologies. More clearly defined exclusions and minimum standards as well as tax exemptions or premium subsidies are also intended to facilitate the implementation of cyber insurance in key industries such as banking and healthcare. It is crucial that education campaigns, mandated by IRDAI and embedded in corporate governance codes, are instrumental in encouraging awareness about the importance of cyber insurance. At the same time, programs aimed at data sharing using anonymized claims databases and building partnerships between private firms and the government are expected to benefit the underwriting process significantly. As far as the development of innovative products goes, it would be beneficial to encourage parametric triggers, cyber resilience add-ons, and insurance products covering emerging risks. Given that cybersecurity remains one of the priorities for the nation, any cooperation between the state agencies and insurance providers should be aligned with relevant cyber security policies developed in India.

VI. Conclusion

In the country, cyber insurance is fast changing from a specialty line of coverage into a strategically critical part of business. The solid basis created through the IRDAI framework is enhanced by the DPDP Act, making it an even more relevant coverage today. Nonetheless, while progress has been made, several aspects, including lack of awareness, lack of standardization, and poor market penetration still hamper the actual utilization of its maximum benefits. As such, in order for the coverage to be maximally utilized, regulation, innovation, and adoption have to be encouraged. With effective regulation and innovative strategies, together with increased awareness regarding the merits of the policy, companies can utilize cyber insurance effectively to improve business resilience. With the current rising trends in cyber risks, companies need to take advantage of cyber insurance as a critical risk management measure. Therefore, to ensure maximum use of the coverage, the gaps in awareness, standardization, and market penetration have to be adequately addressed.

 [ISSN 2581-5369]

VII. BIBLIOGRAPHY

1. Arctic Wolf, *Cyber Insurance: New Coverage Restrictions Expected in 2022*, Arctic Wolf Resources Blog, https://arcticwolf.com/resources/blog/cyber-insurance-new-coverage-restrictions/ (last visited Apr. 20, 2026).
2. Danny Palmer, *What Is Cyber Insurance? Everything You Need to Know About What It Covers and How It Works*, ZDNet (Mar. 5, 2021), https://www.zdnet.com/article/what-is-cyber-insurance-everything-you-need-to-know-about-what-it-covers-and-how-it-works/.
3. *Cyber Insurance Market Size, Growth & Trends Report | 2032*, SNS Insider, https://www.snsinsider.com/reports/cyber-insurance-market-1268 (2023) (forecast period 2024–2032).
4. *Cyber Insurance Requirements in 2024: What You Need to Know*, Intelice Solutions (Jan. 25, 2024), https://www.intelice.com/cyber-insurance-requirements-in-2024-what-you-need-to-know/.
5. *Is It Really Necessary To Have Insurance?*, InternetIsGood (Dec. 2, 2024), https://internetisgood.com/is-it-really-necessary-to-have-insurance/.
6. Payal Wadhwa, *A Complete Guide on Security Incident Management 2026*, Sprinto Blog (Mar. 13, 2026), https://sprinto.com/blog/security-incident-management-guide/.
7. Shauhin Talesh, *Cyber Insurance and Cybersecurity Policy: An Interconnected History*, Lawfare (Nov. 4, 2022), https://www.lawfaremedia.org/article/cyber-insurance-and-cybersecurity-policy-interconnected-history.
8. Sruthy, *Top 10 Cyber Insurance Companies for 2026 [COMPARED]*, Software Testing Help (updated Dec. 21, 2025), https://www.softwaretestinghelp.com/best-cyber-insurance-companies/.
9. *The Legal Implications of Cybersecurity Breaches: Protecting Your Digital Assets*, IP Location (last modified June 8, 2024), https://www.iplocation.net/legal-implications-of-cybersecurity-breaches-protecting-your-digital-assets.
10. *What Is Cyber Insurance? Understanding the Basics of Cyber Insurance. What You Need to Know*, Zenarmor, https://www.zenarmor.com/docs/network-security-tutorials/what-is-cyber-insurance (last visited Apr. 20, 2026).

*****

 [ISSN 2581-5369]