INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBER INSURANCE IN INDIA: NAVIGATING LEGAL FRAMEWORKS

AUTHOR - BOOBESH S, STUDENT AT SASTRA DEEMED UNIVERSITY

BEST CITATION - BOOBESH S, CYBER INSURANCE IN INDIA: NAVIGATING LEGAL FRAMEWORKS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 4 (4) OF 2024, PG. 644-652, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

Cyber insurance, also referred to as cyber liability or cyber risk insurance, defends against internet-based dangers that have emerged rapidly within a couple of years. Cyber insurance coverage went from covering primarily online software in the 2000s into a broad array of risks that consist of network security breaches, unauthorized access, data loss, and even virus-related incidents. The newer threats of data breaches and ransomware and identity theft have emerged as a vital tool in the cyber insurance risk management. However, this is still quite nascent in India-the regulatory changes, such as the 1938 Act of Insurance and the Information Technology (IT) Act of 2000, providing for utterly insufficient resolutions to stand apart against specific cyber risks. The paper will look at cyber insurance in the law structure of India: key drivers and challenges to its growth. It positions the need for legal reforms-including required breach reporting, a comprehensive Data Protection Law, and standardization of cyber insurance policies. This would therefore also strengthen the legal framework, boost confidence in cyber insurance, support the market's growth, and improve the general cybersecurity scenario in the country as these threats continue to evolve.

KEYWORDS - Cyber Insurance, India, DPDP Act, IT Act, Insurance Act.

Introduction

I. Cyber insurance is also known as cyber liability or cyber risk insurance. Cyber insurance is an insurance product that is employed in the protection of businesses as well as individual users from internet-based risks. Its primary objective is to protect users from information technology risks. Cyber threats have evolved very much with time. For instance, in the 2000s, cyber insurance policies significantly covered online software. But the technology, with its systems, has considerably matured to become a volatile and dynamic cyber insurance market. Consequently, the new cyber insurance policies emerged fundamentally resulting from the liability policies for media and software risks. Moreover, it is in the late 2000s that cyber insurance policies began to include issues such as network security, unauthorized access, data loss, and other virus-related issues. Generally, cyber risk insurance policies have featured a number of exclusions. Risks from individuals and businesses in the contemporary digital world are increasing due to the cyber threats occasioned by data breaches, ransomware, identity theft, among others. Cyber insurance is currently some of the most vital aspects of risk management that aids the fight back. Cyber insurance supports businesses in assuming the financial impact of cyber-attacks; however, the trend in India is of recent origin and certainly, regulatory changes such as in the Insurance Act and Information Technology (IT) Act have encouraged its adoption. The paper discusses the role of cyber insurance in India's legal framework, important drivers, challenges, and its probable capacity to reduce cybersecurity risks.

II. Literature review.

Research conducted by Nir Kshetri in "The evolution of cyber-insurance industry and market: An institutional analysis" it states the evolution of how the cyber evolves into the society. It discussed a ransomware attack

which victimized an international food company Mondelez International which affected 1700 servers and 24000 laptops went permanently dysfunctional. It raised a claim with its insurer Zurich American Insurance Company but it rejected it by stating that it was an act of cyber war and it cannot be claimed. And it was not yet decided by the court.

It also stated some other cases that are not decided as being the concept of cyber insurance was undeveloped. It looked at institutions and institutional field in the context of the cyber insurance industry and market. Next, key mechanisms of institutional changes in the cyber insurance industry and market are discussed. It is followed by a section on discussion and implications. The final section provides concluding comments on institutions' effects on the cyber insurance industry and market.

In other research by Manveet Singh discovers the growth of cyber insurance by providing insights that what were the risks and what damages can be happen both in direct and indirect ways. It envisages the role of cyber insurance in mitigating the losses occurred during the breaches and some basic problems with cyber insurance.

The team of authors (Woods & Simpson, 2017) examines the practice of cyber insurance from public-private partnerships. The mutually beneficial nature of the cooperation between cyber insurers and public authorities is noted. The authors analyse the nature of government institutions impact on the functioning of the cyber insurance market.

In research by IIM Calcutta, it describes what are all the major threats in the age of work from home culture. The effect of how pandemic made every person relied on their digital devices making more vulnerable towards the cyber threats. It imposes focus on the making the cyber insurance as a personal insurance to safeguard from the cyber threats.

Alex R Mathew paper addresses how information technology has become part of our daily activities. The organizations were now solely relied upon the computers. Here he gave a basic idea against the term cyber insurance and how it is necessary in this growing digital era.

III. Research Problem.

To focus on the problem of lack of regulatory framework when it comes to regulating the policy drafting and its legal compliances and to deal with the ambiguity in existing legal provisions.

IV. Research Objective.

The aim of the study is to find the clarity over the laws in India covers the Insurance policies and to know the awareness among the businesses and individuals regarding the cyber security Insurance. By comparing the global market and Indian market on cyber insurance the readers will get to know how it has been established in our country.

V. Research Question

i. Whether is there any specific provisions to deal with policy framing?
ii. Whether the legal provisions indirectly imposing mandate to adopt cyber insurance?

VI. Scope and Limitation.

This study analysing the role of Insurance Act and Information Technology Act in regulating and governing the cyber insurance policies. The study's shortcomings include data restrictions, as it is relied on secondary data sources such as case studies and literature reviews. This may make it more difficult for the study to address current trends or acquire empirical validation through data collection from real-world circumstances.

VII. Research Method

This research comprises of literature reviews, which will include a review of academic papers, case studies, and legal analyses. The normative juridical research approach was used to reconcile the legal rules controlling the protection of norms with other legal regulations

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

relevant to the application of legal regulations in the field. A normative juridical study examines library materials, specifically secondary data or legal research undertaken within libraries. It undertaken qualitative focusing on how cyber insurance policies are governed under the Indian legal setup.

CHAPTERS

1. The evolution of cyber insurance

1.1 Global Context

Cyber insurance finds its roots in the increasing cyber-attacks globally. In 1997, Steven Haase approached American International Group Incorporation with the first cyber insurance policy. Digitalization gave more space to cyber-attack and increased ransomware attacks, data breaches, and cyber extortion. It is in this background that many companies across industries ventured into cyber insurance as part of their approach towards risk mitigation. The transformative leadership is being staged by key regions like the US and Europe, where regulatory developments such as the General Data Protection Regulation in Europe have driven the need for mandatory security measures and liability. The global cyber insurance market was valued at USD 16.21 Billion in 2023, North America is the largest cyber insurance market. Cyber Insurance Market: The cyber insurance market is mature globally, and the key players in the sector are AIG, Allianz, and Zurich-all of them offer wide-ranging cyber insurance policies. North America has the largest cyber insurance market primarily due to different regulatory requirements such as HIPAA and CCPA. On the contrary, GDPR has had a huge influence on the European market, forcing companies to protect personal data and putting a very heavy fee in case of its breach. Cyber insurance penetration is rather high among large enterprises in both the U.S. and Europe while policies cover a wide range of cyber risks including data breaches, cyber extortion, and business interruption. Many multinational corporations operating in these areas buy a cover that includes regulatory fines and legal liabilities besides operational losses.

1.2 Cyber Insurance in India

This product was first introduced in 2017. In 2023, Insurers distributed over 300 million policies. Compared to the previous year, it had increased insurance policies by more than 13 percent. IT, BFSI, such as Banking, Financial Services, and Insurance, healthcare, and manufacturing industries have been driving the uptake of cyber insurance. Most of these regulatory frameworks, like the Insurance Act, 1938 and the amendments under the IT Act, 2000, have provided judicial ambiguity in the context of legal backing for cyber insurance policies, which keeps both the insurer and the businesses that got exposed to such cyber risks. India's cyber insurance market remains underdeveloped but has huge potential. Major Indian insurers like Bajaj Allianz, ICICI Lombard, and HDFC ERGO have developed cyber insurance products; however, uptake is relatively low among SMEs. Different from their global peers, Indian enterprises including SMEs consider cyber insurance as cost rather than as a need. Lack of regulatory enforcement remains the primary difference between India and west markets. Though, while GDPR in Europe has been a game-changer such that businesses in significant number have had to invest in cyber insurance, India's regulatory ecosystem is much less mature. Still, Data Protection Bill is in draft form, and penalties for data breaches under the IT Act are not stringent enough to force companies to take preventive measures like buying insurance.

2. Legal Frameworks and Cyber Insurance

2.1 Insurance Act, 1938

The Insurance Act, 1938 governs the insurance policies, providing the legal framework for creating and administering insurance policies. In recent years, insurers have begun offering cyber insurance policies as part of general liability and professional indemnity insurance. These policies are specifically tailored to cover

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

damages from cyber-attacks, data breaches, and digital fraud. But there are no such specific provisions regarding the cyber insurance policies.

2.2 Information Technology (IT) Act, 2000

The primary legislation regulating cybersecurity in India is the IT Act, 2000, amended in 2008. In India, issues like cybercrime, data protection, and privacy are regulated under this act. Under section 43A of the Act, companies liable to pay for compensation in case of failure to implement reasonable security practices and a data breach occurs. This makes businesses adopt cyber insurance as risk mitigating towards its consumer's claim over breaches and threats. This provision is essential for cyber insurance as insurers are mostly looking for cybersecurity measures in companies before underwriting policies. In addition, companies are motivated to enhance their data security practices and hence make them eligible for purchasing cyber insurance policies.

2.3 Digital Personal Data Protection Act

The Digital Personal Data Protection Act, 2023 makes stringent penalties for data breaches and non-compliance to the security measures which are prescribed by the provisions. Those businesses handling sensitive personal information are now indirectly instigated to opt for the cyber insurance policies to mitigate the expenses and losses occurred due to cyber threats.

3. Coverages and Scope

The major coverages were classified into two categories

a. First-party losses: the losses accrued when the firm got breached.
b. Third-party losses: expenses and cost suffered relating to third parties or customers or partners in the event of breach.

India is still developing in framing of policies regarding the emerging cyber threats in day-to-day life. Insurers are covering the losses and expenses of businesses and individuals by covering third-party coverages of the damages, expenses, fines and penalties.

a) Theft of funds – Provides protection in respect of theft of funds due to Cyber Incident or Hacking of insured's Bank account, Credit/Debit card and/ or Mobile wallets by a Third Party.
b) Identity Theft Cover – Provides protection in terms of Defence cost for claims made against insured by third / affected party due to identity theft fraud, provides expense to prosecute perpetrators and other transportation cost.
c) Social Media Cover / Personal social media- Provides protection in terms of Defence cost for claims made against insured by third / affected party due to hacked social media account of insured, provides expense to prosecute perpetrators and other transportation cost.
d) Cyber Stalking / Bullying – Provides expenses to prosecute the stalker.
e) Malware Cover / Data Restoration Cost – Provides coverage for data restoration cost due to malware.
f) Phishing Cover – Provides protection in respect of financial losses as a result of phishing attack and provides expense to prosecute perpetrators.
g) Unauthorised Online Transaction – Provides protection against fraudulent use of bank account, credit / debit card, e-wallet by third party to make online purchasing over internet.
h) Email Spoofing - Provides protection in respect of financial losses as a result of spoofed email attack and provides expense to prosecute perpetrators.
i) Media Liability Claims Cover – Provides coverage for defence costs in third party claims due to defamation or invasion of privacy due to Insured's publication or broadcasting of any digital media content.
j) Cyber Extortion Cover – Provides protection for extortion loss as a result of Cyber

extortion threat and provides expense to prosecute perpetrators.

k) Data Breach and Privacy Breach Cover – Provides indemnity for defence costs and damages in respect of claims lodged by a Third party against the Insured for Data Breach and or Privacy Breach.

4. Challenges in Adoption

4.1 Less Awareness

In growing cyber threats, it makes businesses demand for cyber insurance, but many of the businesses remain unaware of its benefits. The data shows that only 40-50% of policies cover less than USD 5 million. Many Small and Medium businesses are not aware of the benefits and not adopting the cyber insurance policies to get benefit through various coverages. This highlights the need for greater education and awareness.

4.2 Lack of Actuarial Data

The insurers have no actuarial data on cyber attacks as it was emerging in a different shape and involves various damage which makes the professionals to assess and price the policies. This dynamic nature of the cyber threats from phishing to ransomware make more complex to risk analysing compared to risk such as fire and thefts have the data which are fixed not like the evolving cyber risks. There are no legal policies providing the framework for fixing margin regarding the cyber threats.

5. Legal Gaps and Ambiguities

There is no unified law regarding insurance against data protection which makes uncertainties for both insurers and businesses. Even it provides some assists but lacks for the framework regarding data protection, digital payments and e-commerce over individuals. Moreover, global businesses operating in India may face conflicts between local laws and international regulations like GDPR.

a) Compulsory FIR in case of a Cyber incident is a must while filing a claim which becomes a hassle for an individual and creates distrust in their minds when claims are not settled because of the same.

b) Territory and Jurisdiction is restricted to India only in most of the policies. A number of syndicated frauds originate from outside India (e.g. phishing, ransomware, malware attacks), cyber insurance clauses may or may not be clear on the coverage in this regard.

6. Recommendations

6.1 Policy Enhancements

Cyber insurance must be customized to meet the specific needs of each business. For example, an insurer can give a pre-breach assessment for a business. Such assessment can help a business understand what is lacking and prevent breaches. Coverage on GDPR-related fines for international businesses should be a great initiative for insurers**.**

6.2 Awareness and Training

Governments and the industry bodies can make efforts to mount awareness campaigns about cyber insurance. Training programs for businesses on financial and legal implications of cyber risks will help raise acceptance among sectors. Some of the initiates that are most likely to be helpful in improving adoption rates come at the level of SMBs, which are much more susceptible to cyber-attacks.

6.3 Strengthening Legal Frameworks

This can only be achieved by having the passage of Data Protection Bill and updating the IT Act, based on the current cyber risks that it should cover. A single regulatory framework will help inform clarity to businesses for the purpose of investing in comprehensive cybersecurity measures and insurance coverage.

Case Studies

1. **AIIMS Cyberattack (2022-2023):**

In November 2022, India's premier healthcare institution, All India Institute of Medical Sciences (AIIMS), was hit by a big ransomware attack. Hackers encrypted essential patient data at

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

AIIMS, and this crippled hospital operations for nearly two weeks. The hackers asked for a ransom to unlock the encrypted data; no ransom has been reported to have been paid, but this attack did gain serious attention over the vulnerability of India's critical infrastructure. Recovery was long-drawn and involved incurring huge financial and reputational losses for the institution and the government as a whole. The incident of AIIMS necessitated the need for cyber insurance cover in the health sector, especially concerning the pecuniary costs arising from downtime and data recovery expenses. Secondly, having ransomware protection in cyber insurance policies would cover the ransom itself and the costs of restoring compromised systems. The attack also prompted government reconsideration of its cybersecurity policies and encouraged institutions to embrace cyber insurance in curbing such outcomes.

2. **Cosmos Bank Cyber Heist (2018):**

The cyber heist involving Cosmos Bank in 2018 stands today as one of the greatest cyberattacks India has ever witnessed. Hackers managed to siphon off ₹94 crore from the bank's system via a malware attack on its ATM switch system. The attackers, besides carrying out several fraudulent transactions, cloned many cards and retrieved SWIFT systems. After this happened, huge financial losses were realized, and although the bank recouped some of the stolen funds, the move highlighted the need for insurance coverage in dealing with cyber actions to prevent financial fraud. In this case, cyber insurance would cover financial loss resulting from the theft and expenses incurred in investigating the breach, restoring affected systems, and alerting affected customers. Indeed, for banks and other financial houses, covering cyber insurance policies through fraud protection is really a must because these organizations are always targeted by cyber criminals.

3. **Microsoft Outages (2024):**

In 2024, Microsoft faced a series of outages caused by DDoS attacks. Such outages hit critical services like Outlook, Teams, and Azure, affecting global businesses. Although there were rumors that Microsoft did not pay any ransom, the attacks sent a wave of unease among businesses relying on third-party service providers. Business losses occurred due to such outages, and it made companies look back at cyber insurance policies. For third-party-dependent business firms like Microsoft, coverage for the business disruptions resulting from outages or failures can form part of their cyber insurance policies. With this, companies can recover lost revenue generated from their downtime as a result of critical software or cloud services. Third-party liability coverage will also be used to address potential legal claims due to a service provider's breach on its SLAs.

4. **Zomato Data Breach (2017):**

For example, in 2017, one of the biggest food delivery platforms in India, Zomato, faced a data breach from hackers resulting in the theft of private information of 17 million of its users. The payment details were not exposed, but usernames, email addresses, and hashed passwords were exposed. The firm acted quickly and immediately contained the breach and negotiated with the hacker, but the reputational damage remained associated with such an incident. This case illustrated why cyber insurance would be relevant to Zomato in protecting reputational damages, adding legal fees and costs of notice for affected users. Beyond compensation in monetary value, Zomato would have also enjoyed policies providing cover for public relations costs playing a part in rebuilding consumers' confidence.

5. **WannaCry Ransomware Attack (2017):**

The WannaCry ransomware attack in 2017 had taken over various organizations across India, mostly organizations in the healthcare and telecom sectors. These malware locked users

out of their systems and demanded Bitcoin payments to restore access. This incident showed how vulnerable the organizations were without adequate cybersecurity measures. Cyber insurance coverage can become useful in case of ransomware attacks by covering payments, costs of data recovery, and business disruption losses for the organisations. This coverage saves companies from significant financial losses due to the lost downtime as the companies can quickly resume their operations following an attack by ransomware.

6. **Haldiram's Ransomware Attack (2020):**

Just recently, in 2020, snacks maker Haldiram's suffered a ransomware attack by hackers requesting ransom in Bitcoin. Its data got encrypted, causing enormous operational disturbances. Cyber insurance would have been important in this case by paying the ransom as well as taking into account the expenses related to restoring the encrypted files. Another thing that is included in cyber insurance policies is business interruption coverage, which would help deal with financial loss experienced because of the downtime caused by attack

8. Legal barriers

8.1 High Premium Costs

Being there is no transparent provision regarding the establishment of margin premium cost, the high level of premium cost is one of the main barriers to the adoption of cyber insurance, especially for SMEs. The premium cost depends entirely on the company's risk profile, where factors such as company size, the kind of data handled, and the strength of its cybersecurity infrastructure are all considered. Many SMEs, with typically an already thin margin, find cyber insurance premium costs far too expensive.

8.2 Lack of Cybersecurity Infrastructure

Indian small and medium-sized enterprises lack proper cybersecurity infrastructure, which makes them a high-risk for insurers. Most businesses are not equipped with a full security framework set up that includes a firewall, multi-factor authentications, and data encryption, which heightens the risk of cyberattacks. Without such controls, they hesitate to write or charge extremely high premiums for cyber insurance and deter businesses from purchasing cyber insurance.

8.3 Insufficient Claims Experience

The Indian market for cyber insurance is still in the development process and lacks sufficient claims experience. The availability of historical data on frequency and severity of cyber-attacks is limited to insurers, which further makes it complicated while conducting underwriting processes. The dynamic nature of cyber threats that range from basic phishing attacks to complex ransomware attacks makes it even more challenging for the insurers to precisely predict the risk involved, subsequently translating into higher premiums and limited options in terms of coverage.

9. Recommendations

9.1 Evolving Risk Landscape

As India's digital economy expands, the risk landscape will change and add new security challenges created by emerging technologies like blockchain, AI, and IoT. For example, an industrial IoT network in the manufacturing sector would come under large-scale cybercrime attacks due to its critical infrastructure. The corresponding cyber insurance policies would have to assume new types of risks created by these technologies.

9.2 Developing Standardized Policies and

The absence of standardized cyber insurance policies is a significant issue in India. Each insurer currently offers highly customized policies, leading to confusion among businesses. Developing standardized policies, much like those for traditional insurance (e.g., fire or motor insurance), would help streamline the purchasing process encourage broader adoption, particularly among SMEs.

9.3 Collaboration Between Industry and Government

The cooperation between the insurance industry, cybersecurity experts, and the government in India would need to be enhanced for cyber insurance to grow properly. Awareness campaigns backed by the government, industry certifications for the measures of cybersecurity, and a central repository for data on cyber-attacks would help reduce uncertainty in pricing and encourage investments from businesses to secure cyber insurance. The government can consider providing tax incentives to organizations that purchase cyber insurance, just as is being done for health insurance. While it would indeed make Indian businesses' cybersecurity posture better, it would also ultimately contribute to a more resilient digital economy.

9.4 Strengthening Legal Frameworks

Legal framework must be strengthened to encourage the growth of this cyber insurance market. Passing the Data Protection Bill is a critical landmark step in this regard. IT Act must be amended to include explicit provisions pertaining to cyber insurance, like mandatory breach reporting for insured businesses as well as penalties for failure to report.

Conclusion

While cyber insurance is gaining momentum in India, in its current form, the legal framework does not support it well enough. The Insurance Act of 1938 covers general insurance but has no provisions specific to the nature of cyber risks. Even the IT Act of 2000 has unclear provisions related to liability, data breaches, and claim settlements, and such provisions are necessary for insurance policies, especially those of cyber insurance. There is also no All-inclusive Data Protection Law, leaving a gap in the regulation of data security and reporting breaches. Legal updates are required to increase the level of trust among stakeholders, thereby raising adoption. These updates can include mandated breach reporting, a single data protection law, and homogeneous cyber insurance policies. A more stringent legal framework would not only stimulate growth in the cyber insurance market but also enhance India's cyber security in general. Updating these laws is important to provide adequate protection and guidance for businesses and insurers in this rapidly evolving phase of cyber threats.

References

1. Bandyopadhyay, Mookerjee, V. A model to analyze the challenge of using cyber insurance. *Inf Syst Front* **21**, 301–325 (2019).
2. Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, *52*(11), 68-73.
3. Böhme, R. (2005, June). Cyber-Insurance Revisited. In *Weis*.
4. CALCUTTA, I., & India, F. (2021). It's time for cyber-insurance to become personal in the WFH age.
5. CYBER INSURANCE IN INDIA Mitigating risks amid changing regulations & uncertainties by Data Security Council of India.
6. Cyber security insurance policy by IFFCO Tokyo general imsurance company private limited.
7. Ismail, N. (2017). The era of Cyber-attacks: AI's role in cyber insurance. [online] Information Age.
8. Kalra, K., & Tanwar, B. (2023). Cyber security policy in India: Examining the issues, challenges, and framework. In *Cybersecurity issues, challenges, and solutions in the business world* (pp. 120-137). IGI Global.
9. Kshetri, N. (2019). The economics of cyber-insurance. *IT Professional*, *20*(6), 9-14.
10. Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. *Telecommunications policy*, *44*(8), 102007.
11. Kurmaiev, P., Seliverstova, L., Bondarenko, O., & Husarevych, N. (2020). Cyber insurance: the current situation and prospects of development. *Amazonia Investiga*, *9*(28), 65-73.

12. Matthew, A. (2019). Cyber Insurance. International Journal of Engineering and Advanced Technology, 8(6), 47-51.
13. Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers*, *21*, 997-1018.
14. Mukhopadhyay, A., Saha, D., Chakrabarti, B. B., Mahanti, A., & Podder, A. (2005). Insurance for cyber-risk: A Utility Model. *Decision (0304-0941)*, *32*(1).
15. Nishanka, A. K. (2016). Evaluating Cyber Infrastructure for Cyber-Insurance in the Corporate World: An Analytical Focus. *Available at SSRN 2864383*.
16. Report of the Working Group to study Cyber Liability Insurance on Individual Cyber Insurance.
17. Section 43A of the Information Technology Act, 2000.
18. Singh, M., & Arora, A. P. (2017). Perspective and Growth of Cyber Insurance. *World Journal of Research and Review*, *4*(6), 61-64.
19. The Digital Personal Data Protection Bill, 2022
20. The Insurance Act, 1938