CYBER LIABILITY INSURANCE - THE FUTURE OF CYBER SECURITY IN INDIA

Mr. Aniket Rai, Assistant Professor, School of Law, IMS Unison University, Dehradun | LL.M, NLSIU Bangalore | BA.LLB, U.P.E.S Dehradun

ABSTRACT

As per the recent estimates of Ministry of Home Affairs (MHA), India lost around Rs. 7000 Crore to online fraud in the first half of this year. This figure is alarming for a country which has the third most digitized population in the world. It is also concerning because India is still finding a way towards attaining a full-proof cyber security mechanism.

This article is an answer to the high financial risks that the Indian Population currently faces through cyber-attacks. It introduces readers to the future of cyber security, which is "Cyber Liability Insurance".

"Cyber Liability Insurance" is not a new concept and has acquired relevance since the early 21st century in the world and in India too, but the problem lies in allotting priority to this cyber resilience mechanism which may prove a game-changer in attaining optimum cyber security landscape.

This insurance mechanism is different from general insurance policies and not only focuses on financial indemnity amid cyber threats but also gives due importance to the cyber-attack prevention mechanism and the business restoration activities in case of contingencies. In India, there are certain insurers that are offering cyber insurance but there is a lack of knowledge eco- system that could ensure proper guidance to the prospective buyers.

This gap has led to the emergence of a population which is not aware of the technicalities of cyber insurance and in case of being aware, not eligible to make appropriate choices for themselves. Hence, in this work the author has tried to introduce "cyber liability insurance" to the readers by simplifying its concepts and various terminologies. Also, a comparative analysis has been made with the legislative and regulatory framework that surrounds this market in USA and Europe.

There has been literature which deals with cyber insurance, but while some of them have just incidentally touched upon this context, others have been from a technical perspective.

This article is one of the only works that has comprehensively dealt with the state of Cyber Insurance in India vis-a-vis a socio-legal point of view.

The paper has also borrowed certain empirical studies to prove the hypothesis that 'prevention' alone is not the best option towards cyber security and 'preparation' as well as 'mitigation' is the future of cyber security.

Keywords: Cyber Liability Insurance, Cyber Attack, Online Fraud, Cyber Resilience, Indemnity.

Introduction

In a technology driven world, 'Data' and 'Cyber Security' are co-existent as a concept. The technological revolution has not only made the world an easy place to live but also an easy place to fall prey to a *guilty mind.*

In the world of electronic gadgets, data is a "two- edged sword" and its use or misuse solely lies with the beholder and therefore to minimize the volatile or uncertain nature of 'data', 'cyber security' is used as a shield.

'Cyber Security' means *protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.*[1]

In simple words, 'cyber security' is a combination of various electronic processes which secures an individual's data from the outside world and in the absence of a cyber security framework an individual's data is unsafe and is open to any kind of unauthorized use, which may curtail an individual's privacy and may expose him to risks. The gravity of these risks may depend on the nature of information contained in the data.

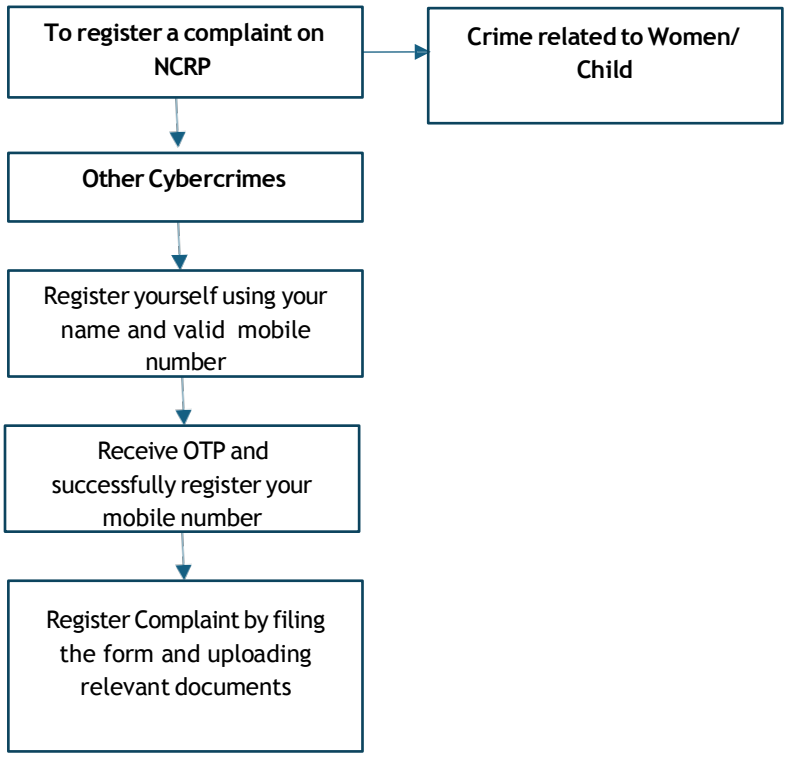
Legislative and Administrative Set-Up against Cyber- Crime in India

The Government of India has a comprehensive legislative as well as administrative framework that defines its institutional fight against cyber-crimes. One recent initiative with which most of us

[1] Information Technology Act 2000, s 2(1)(nb)

are aware is the "caller tune awareness initiative" joined by Megastar Amitabh Bachchan, in which he alerts a caller against cyber fraud and probable risks, in the meantime a call is connected.

In India, there are around 10 regulations[2] at the Central level which includes legislations, policy documents and rules- regulations as well as guidelines that deals with cyber- security. Further, these regulations are supplemented by certain "sector-specific regulations" [3] and "state-level regulations"[4] as well.



[2] Information Technology Act 2000, CERT-In directions under Section 70B, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018, The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code Rules, 2021), The Digital Personal Data Protection Act 2023, National Cyber Security Policy 2013, The Aadhaar (Data Security) Regulations 2016, Meghraj Policy – Cloud Security Best Practices, National Information Security Policy and Guidelines (2019)

[3] CEA (Cyber Security in Power Sector) Guidelines 2021, Draft CEA's Regulation Measures on Cyber Security in the Power Sector 2024, The Reserve Bank of India (RBI) Cyber Security Framework in Banks 2016, RBI Master Direction on Outsourcing of Information Technology Services (April 10, 2023), Draft Telecommunication Cyber Security Rules 2024, Draft Telecommunications (Critical Telecommunication Infrastructure) Rules 2024, MeitY Cloud Empanelment Guidelines, SEBI Framework for Adoption of Cloud Services, SEBI Cyber Security and Cyber Resilience Framework, IRDAI Information Security and Cyber Security Guidelines 2023, PFRDA: Circular on Information and Cyber Security Policy Guidelines - 2024 for Intermediaries/Regulated Entities

[4] Maharashtra Cloud Computing Policy 2018, Assam Cyber Security Policy 2020, , Uttar Pradesh Information Security Policy, Telangana's Cyber Security Policy 2016, Madhya Pradesh's Cloud Adoption Framework 2022

Figure I: Flowchart of the complaint registration process on National Cyber Crime Reporting Portal

One the other hand, we have Indian Cyber Crime Co-Ordination Centre (I4C), under the aegis of Ministry of Home Affairs (MHA), which acts as a nodal agency to tackle cyber-crime, It has eight vertical units working under it, including National Cyber Crime Reporting Portal (NCRP) which is the first point of contact of I4C with a cyber-crime victim. NCRP is a complaint registering portal which brings the jurisdictional police into action. In addition to this, a toll-free number "1930" has been launched as a cyber-crime helpline number.

Fighting against Cyber Threats v. Showing resilience from Cyber Threats

The first quarter of twenty first century has so far witnessed huge technological advancements with the latest inventions being Artificial Intelligence (A.I.) and cloud computing[5], and every step that is taken towards innovation raises concerns over cyber security challenges that it may pose.

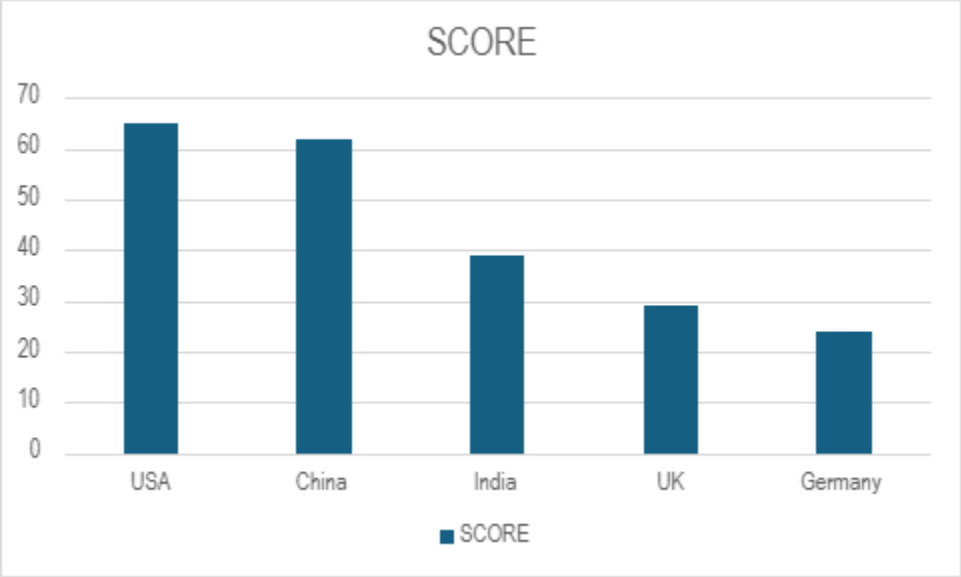


Figure II: Graphical Representation of Top- 5 digitized economy of the world

[5] Munich Re, 'Global Cyber risk and Insurance Survey 2024' *(Munich Re,* 26 April 2024*)*<https://www.munichre.com/en/insights/cyber/global-cyber-risk-and-insurance-survey.html#download> accessed 08 July 2025.

India's digital economy contributed 11.72% to the national income in the FY 2022-23[6], and as per a study of Ministry of Electronics and Information Technology[7] it is expected to grow twice as fast as rest of the economy, thereby reaching 13.42% of the national income by the end of this financial year. Further, contributing to one-fifth of the national income by 2029-30. It is also to be noted that, India is the third largest digitized economy[8], and therefore the stakes are high.

The "State of India Digital Economy Report 2024"[9], which measures the level of digitization in India based on C (Connect)- H (Harness)- I (Innovate)- P (Protect)- S (Sustain) model, finds India low in terms of its 'preparedness against cyber attacks', 'cyber-attacks' and 'trust'. Hence, ranking it low on the standards of Protect (P). Therefore, it becomes necessary to focus on the protection mechanism that can protect our current and future digital atmosphere.

Also, a global survey done by an internationally recognized insurance company, *Munich Re[10],* has led to surprising results. It found that **88% of the participants in India** were extremely concerned about cyber-attacks (even after taking appropriate cyber security measures). India was on second to **Spain** in terms of apprehension of cyber-attacks.

The popular opinion that is often propagated by various Governments across the globe is that Cyber Crimes can be controlled by way of "awareness initiatives", "preventive steps" and "curative steps" taken later by the law enforcement agencies.

This opinion is beneficial to some extent because the public knows about healthy cyber security habits, but in the long run it is faulty as rapid advancement in technology provides new cyber space to the attackers and mere awareness is not enough. The alarming rise in the rate and magnitude of cyber-attacks speaks for itself.

---

[6] PIB Delhi, 'Future Ready: India's Digital Economy to Contribute One-Fifth of National Income by 2029-30' *(Press Information Bureau,* 28 January 2025*)* <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2097125> accessed 08 July 2025.
[7] Indian Council of Research on International Economic Relations, *Estimation and Measurement of India's Digital Economy* (Report, January 2025) Executive Summary.
[8] Deepak, M., Mansi, K., Aarti, R., Krithika, R., and Mayank, M, *State of India's Digital Economy (SIDE) Report, 2024* (2024, Indian Council for Research on International Economic Relations) 05, 17.
[9] Deepak, M., Mansi, K., Aarti, R., Krithika, R., and Mayank, M, *State of India's Digital Economy (SIDE) Report, 2024* (2024, Indian Council for Research on International Economic Relations) 17-30.
[10] Munich Re (n 2).

It is to be noted that many findings have pointed out[11] that achieving "zero cyber-crime" is a myth and therefore focus should be on "cyber- resilience" i.e. *to prevent, withstand and recover from cybersecurity incidents*[12].

Cyber Resilience is a concept which focuses not only on prevention of probable cyber-attacks but also allows preparation for unfavorable situations that may arise in these uncertain times. Hence, focusing on curative measures as well. "Cyber Liability Insurance" is one of the reliable cyber resilient mechanisms.

Cyber Insurance as a means of Cyber Resilience

In India, 'insurance contracts' come under the ambit of both "indemnity contract" as well as "contingent contract", but since section 124 of the Indian Contract Act 1872[13] is restricted to cover only those losses that are caused by a 'person'. Therefore, insurance contracts in India are not strictly dealt by section 124 but still works on indemnity principle.[14]

In insurance contracts, an insurance holder (insured) gets indemnity for any unforeseen loss or damage that may be caused to his/her person or property in the future, from an insurer (insurance company)[15].

Cyber Insurance Policy is an element of "cyber risk management" and involves 'assessing cyber risk', 'adopting mitigations' and 'creating recovery processes'. Data Security Council of India (DSCI) describes cyber insurance as-

"Cyber Insurance is designed to guard businesses from the potential effects of cyber-attacks. It helps an organisation mitigate risk exposure by offsetting costs, after a cyber-attack/breach has happened. To simplify, cyber-Insurance is designed to cover the fees, expenses and legal costs

[11] Yong Yick LEE, Robert J. Kaufmann & Ryan Sougstad, 'Profit-maximizing firm investment in customer information security' (2011) Decision Support Systems 51 (4).
[12] Ministry of Electronics and Information Technology, 'National Cyber Security Policy' *(MEITY,* 02 July 2013*)*<https://www.meity.gov.in/static/uploads/2024/02/National_cyber_security_policy-2013_0.pdf> accessed 08 July 2025.
[13] Indian Contract Act 1872, s. 124
[14] Dinshaw Fardunji Mulla, *The Indian Contract Act* (16th edn, LexisNexis 2019); W Courtney, 'Indemnities and the Indian Contract Act 1872' (Manupatra) http://docs.manupatra.in/newsline/articles/Upload/78F904F2-E9A9-4BA3-9748-09C42A63621E.pdf
[15] Insurance Act 1938.

associated with cyber breaches that occur after an organisation has been hacked or from theft or loss of client/employee information"[16]

Generally, cyber insurance coverage offers "cyber security" as well as "financial indemnity" in case of any financial loss or consequential cost. Hence, ensuring a safe cyber space for the insured. In simple words, it works for the best of the insurer but at the same time also prepares them for the worst. As a result, in recent times "cyber insurance" has become quite instrumental in sustaining organizations against cyber-attacks.

In this context, the latest report of *World Economic Forum "Global Cybersecurity Outlook 2025"* is of essence as it states that size of global market for cyber insurance which was at $ 14 billion in 2023 shall become a business of $29 billion by 2027[17].

Recently an investigative journalism by the Indian Express Newspaper[18] found that wealthy Indian population has become a prime target of digital arrests and though I4C has been quite instrumental in initiating action against the cyber-attacks but only one out of all the surveyed victims was able to recover at least 75% of defrauded amount (see Table I). On discussion with certain cyber experts[19], "Cyber Insurance" is being recommended as a vital tool in attaining optimum cyber security.

Name of the Victim	Amount defrauded	Amount recovered	Time since cyber attack
Mr. S.P. Oswal	Rs. 7 Crore	Rs. 5.27 Crore	9 months
Mr. Biren Yadav	Rs. 1.59 Crore	Rs. 16.1 Lakh	12 months
Mr. Krishna Das Gupta	Rs. 83 Lakh	Nil	15 months

[16] Insurance Regulatory and Development Authority of India, Annual Report 2022–23 (IRDAI, 2023) <https://irdai.gov.in/document-detail?documentId=976463> accessed 14 July 2025.
[17] World Economic Forum, *Global Cybersecurity Outlook 2025* (Insight Report, January 2025) 27 https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.
[18] Ritu Sarin, 'Little or Zero Recovery: Why Money Lost in a Digital Scam Falls Down a Black Hole' The Indian Express (New Delhi, 1 July 2025) 1.
[19] Sundareshwar Krishnamurthyand (Partner- Cybersecurity, PwC India); Lt General (Dr) Rajesh Pant is a globally acknowledged expert in the field of Cyber Security. He previously served as the National Cybersecurity Coordinator in the Prime Minister's Office of the Government of India, TAC Security, 'Lt. General Dr. Rajesh Pant' <https://tacsecurity.com/team/lt-general-dr-rajesh-pant/> accessed 14 July 2025.

Publishing Professional from Noida	Rs. 84 Lakh	Rs. 14 Lakh	No data
Delhi-based scientist	Rs 51.45 Lakh	Rs. 20	No data

Table I: Tabular representation of the surveyed cyber-attacks victims and extracted information

Further it is to be noted that, in the study conducted by *Munich Re "*Global Cyber Risk and Insurance Survey" it was observed that 41% of the surveyed are considering taking cyber insurance soon, as part of their risk management initiatives. The awareness around cyber insurance has also seen a rise among the companies, and now more people are aware of it.

Cyber Insurance Policy- Scope and Extent of Operation

Cyber Risk is one such area where the perception of risk diverges from reality of risk, and therefore an organization that has opted for cyber insurance policy cannot be complacent just because it has insurance. In simple words, cyber insurance policy cannot be treated just as a curative measure because it involves stages of supervision, security and management of cyber space- and indemnity is not the only part of cyber insurance coverage.

A cyber insurance policy usually involves the insured (buyer), broker, insurance company (insurer), reinsurer and cyber security product/ service provider. In most jurisdictions, buyer reaches out to a broker, who analyses the risk and the monetary power of the client based on his "economic status" and the "cyber evaluation" conducted by a tech company.

When a broker suggests an insurer and the buyer reaches out to it, the insurer conducts a "cyber risk assessment" of the buyer through a questionnaire. The buyer may also employ a third party to do its own cyber evaluation. Later, sending its quotation.

When a person buys a cyber- insurance policy, he is bound by the terms & conditions of the policy and therefore the policy document becomes the mother document. Any right or relief which is not part of the policy cannot be claimed. Therefore, it is important for the parties to see what they agree to. Now a days the buyers have been given the flexibility to add on the coverages they are willing to include and at the same time exclude the irrelevant portions, based on their risk assessment.

Usually, a cyber insurance policy covers the following expenses-

1. **Response to breach events:** notification, call center services, breach resolution, mitigation services, public relations, and crisis management
2. **Regulatory coverage:** Costs for notification, defense, penalties
3. **Liability coverage:** Privacy, security, multimedia liability
4. **Cyber extortion and deceptive fraud transfer**
5. **Institution's loss of income or extra expenses:** due to security breach including third parties, system failures, voluntary shutdown of systems following an attack
6. **Data replacement/recovery costs**[20]

Any cyber insurance policy is majorly judged on its nature and extent of coverage because in case a future cyber-attack is not covered under the policy, a company may face consequences of complete closure of its business[21].

A well- planned insurance policy allows an organization to continue its usual business activity, post- cyber incident and therefore "restoration of normal business activity" becomes another important component of the policy which also needs to be seen and analyzed while entering into such agreement. Since, even temporary termination of business activities may cause billions to some companies and therefore ensuring business continuity even in times of adverse environments becomes important.

Further, the purpose of a cyber insurance policy can be fulfilled only if the procedural and regulatory mechanisms aid the cyber insurance environment of a country. This can be done by creating a fast and efficient mode of identifying and raising claims before the insurance company. Since knowing the veracity of the alleged cyber-attack (on time) is indispensable in initiating the claim process. To streamline this process, an online government cyber reporting portal can be created which can certify a cyber-attack to the insurance company so that claim process can be initiated.

Cyber Insurance Policy- Exclusions and Challenges

[20] Data Security Council of India, *Cyber Insurance in India* (2023) <https://www.dsci.in/files/content/knowledge-centre/2023/Cyber%20Insurance%20In%20India-doc.pdf> accessed 14 July 2025.

[21] IAEME, International Journal of Civil Engineering and Technology, vol 10, issue 5 <http://iaeme.com/Home/issue/IJCET?Volume=10&Issue=5> accessed 14 July 2025.

Though cyber insurance coverage includes "cyber mitigation" as well as "risk transfer components", but rarely do the insurance companies focus on cyber security procedures in the contract, as they believe that covering expenses post incident is more effective than mitigating risks in advance.[22]

The "Exclusion clauses" of any insurance policy cover those conditions or situations during which an insured cannot claim insurance. The exclusion clauses in cyber insurance policy play a vital role in determining coverage. Some of the common exclusions include cyber warfare, lack of pre-assessment framework, non-malicious events such as 'mistake' and 'omissions' by the insured, physical or infrastructural damage. These exclusions are common in insurance contracts found across the globe.

There are certain challenges in the cyber insurance sector as well, which are affecting the insurers as well as insured globally-

1. **Pricing**- Pricing of the insurance policy is a challenge because there is a lack of adequate historical data dealing with cyber-attacks [23], and therefore the pricing of premiums is predominantly based on expert models developed by way of cyber risk assessment[24].
2. **Business Continuity and Waiting Periods-** In cyber space, business continuity is a key and any disruption caused by cyber-attack may cause billions of dollars. Therefore, reducing downtime is an aspect on which cyber insurance policies need to work.
   In IT Services[25], availability of an organization is measured by the number of "nines" i.e. 99.9% availability is three nines, and it refers to below 9 hours of downtime for all outages in a year, while 99.99% is four nines[26]. Still, the waiting period found in standard cyber insurance policies is never shorter than 6 or 8 hours for a single outage. In simple words, for an insurer to claim insurance its outage must exceed 6 or 8 hours to get coverage under the policy. This is a big concern for the insured, as they have to wait until their downtime exceeds the waiting period provided under the policy.

---

[22] *ibid.*
[23] European Union Agency for Network and Information Security (ENISA), Incentives and Barriers of the Cyber Insurance Market in Europe (Technical Report, ENISA 2012 <https://www.enisa.europa.eu/publications/incentives-and-barriersof-the-cyber-insurance-market-in-europe> accessed 14 July 2025.
[24] *ibid.*
[25] J Rapoza, Preventing Virtual Application Downtime (Technical Report, Aberdeen Group 2014).
[26] Service level agreements with three nines or better are very common

3. **Lack or no cyber security mechanism-** The insurers are not willing to extend their policy to people or organization who have no or poor cyber security mechanism as providing insurance to this category of people may put them in a vulnerable position in which they may incur frequent claims and huge losses.
4. **Lack of awareness** is also one of the components that has affected the cyber insurance industry at large.
5. **Rapid advancement of technology and its volatile nature** also adds to the problem of insurance companies.

At this stage, we have a substantial understanding of "what cyber insurance is" and "how it works". It becomes important to refer to certain countries where cyber insurance is on boom.

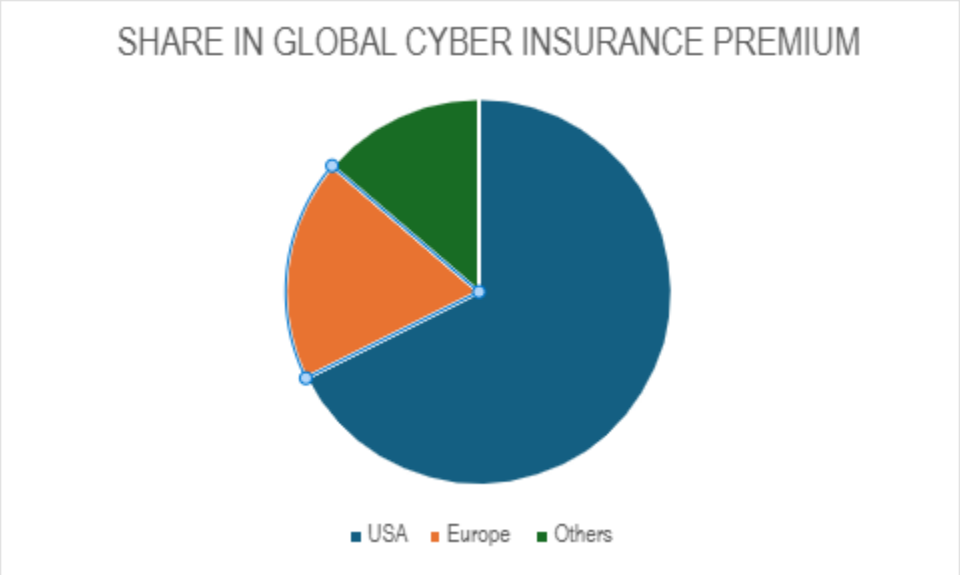


Fig III: Pie-Chart indicating the state of Global Cyber Insurance Market

In this regard, it is to be noted that USA dominates the world cyber insurance market with around 69% of global cyber insurance premiums[27] going in its hands. While Europe accounts for 19% of the global cyber insurance premium.

Cyber Insurance Framework in U.S.A

[27] Swiss Re, 'Reality Check on the Future of the Cyber Insurance Market' (Swiss Re, 18 November 2024) <https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/aboutcyberinsurance-market.html> accessed 14 July 2025.

USA is a world leader in the cyber insurance market, and the reason behind it is the early initiatives taken by the US Government in the cyber security landscape. In the year 1996, under the Presidentship of Mr. Bill Clinton the country established a "Commission on Critical Infrastructure Protection" to protect infrastructures against cyber threats.

Further in 1999, the Federal Financial Services Modernization Act was enacted which imposed an obligation on financial institutions to protect sensitive data of consumers and ensure transparency while sharing their data with third parties. Since, the cyber-attack cases saw a continuous rise, U.S. Securities and Exchange Commission issued guidelines in the year 2011 requiring publicly traded companies to include and discuss cyber risk as another business risk item in their annual filings.

As of 2018, all 50 states including the District of Columbia require private and government entities to inform the public when they experience a data breach. In practice, firms disclose breach-related information to the attorney general's office in their respective states. Further, the entities are also liable for monetary fines and penalties (as per the laws of the States) in case a breach is detected.[28]

In USA, National Association of Insurance Commissioners (NAIC) is the regulatory body that sets standards and provides expertise, data and information to insurance commissioners for effectively regulating the industry and protecting the consumers. NAIC conducts timely study on the status of cyber insurance industry in the country and points out various lapses in the system and required changes that need to be made. The report titled "Report on the Cyber Insurance Market[29]" provides historical data to the regulators and industry on a yearly basis, which ultimately helps them to fill the existing gaps in their policies accordingly.

Further, they have also developed a regulatory database by the name "SERFF Database[30] i.e. System for Electronic Rates and Forms Filling Database", which provides access to all policy documents (submitted to regulator) including- insurance policy final draft, application form and

[28] IT Governance USA, Data Breach Notification Laws by State (IT Governance USA, July 2018) <https://www.itgovernanceusa.com/data-breach-notification-laws> accessed 14 July 2025.
[29] National Association of Insurance Commissioners (NAIC), Report on the Cyber Insurance Market (Memorandum to Members and Interested Regulators of the Property and Casualty Insurance Committee and Innovation, Cybersecurity and Technology Committee, 15 October 2024) <https://content.naic.org/sites/default/files/cmte-h-cyber-wg-2024-cyber-ins-report.pdf> accessed 14 July 2025.
[30] National Association of Insurance Commissioners (NAIC), *SERFF: Modernization* (web page, published March 3 2025) <https://www.serff.com/serff_modernization.htm> accessed 14 July 2025.

pricing mechanism. It has developed into a convenient platform for consumers to pick and choose appropriate insurance policies as per their priorities.

Since in the US, there has been a strict legislative mechanism which is complemented by a trust-worthy regulatory set up. Therefore, industries in the USA usually opt for cyber insurance. Hence, resulting in the country being the hub of the cyber insurance industry.

Cyber Insurance Framework in Europe[31]

EU started its journey of prioritizing cyber security in 1995 by issuing the European Data Protection Directive. But unlike the USA, it took around two complete decades for Europen countries to adopt a comprehensive legislation having binding effect. As it was in 2014 that the European Parliament passed "General Data Protection Regulation (GDPR)[32]", thereby imposing a duty on every organization to take cyber security measures for protection of consumer data.

Further, they also came up with EU Cybersecurity Act in 2019[33] and introduced "cybersecurity certification framework" which helps the organizations operating in Europe to prevent and detect cyber incidents and helps them to record such incidents and recover from them in a timely manner.

Within the GDPR framework, data protection violations are subject to substantial fines and penalties. These fines are designed to be proportionate and dissuasive for each incident and can be up to €20 million (a minimum of €10 million for less severe incidents), or, in terms of an undertaking, 2-4% of their global turnover depending on the severity[34]. This had a deterrent effect and led to the emergence of the cyber insurance market in Europe which is growing stronger and stronger as organizations want to ensure their financial stability as well as business continuity in times of cyber-attacks.

Cyber Insurance Framework in India

[31] By the term "Europe" author here means "European Union (EU)", which is a political and economic union of 27 member states.
[32] GDPR-Info, EU General Data Protection Regulation (GDPR) (GDPR-Info, last updated 2024) <https://gdpr-info.eu/> accessed 14 July 2025.
[33] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act) (EU, OJ L 151/15, 7 June 2019) (amended, consolidated version 4 February 2025) <https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng> accessed 14 July 2025.
[34] GDPR (n 44).

In India, the Information Technology Act of 2000 and Digital Personal Data Protection (DPDP) Act of 2023 majorly governs the cyber security mechanism. Especially after the coming up of DPDP Act 2023, an obligation has been imposed on data fiduciaries to protect the personal data of their users, otherwise face penalties.

Under DPDP Act, a data fiduciary has been made obligatory to protect personal data under its possession or control by adopting "reasonable security safeguards" to prevent any kind of breach[35]. Further, it is bound to inform the Data Protection Board of India (DPBI) in case of any breach[36]. In the case of Significant Data Fiduciary, the rules are stricter, and they are duty bound to conduct timely data audit and undertake "periodic data impact assessment"[37].

The Schedule[38] annexed to DPDP Act lays down fines and penalties for data fiduciary in case of breach of any obligation imposed by the Act. For instance, failure to take "reasonable security safeguards" for protecting personal data of users can cost up to Rs. 250 Crores to an entity. While, failure to inform the authorities about data breach may cost up to Rs. 200 Crores in penalty.

After the coming up of the act of 2023, the data fiduciaries are under a duty to protect their data by taking appropriate steps, and therefore an economic aspect has come into play with penalties ranging from hundreds of crores. Since the stakes are now high in India as well (in case of data breach), therefore "Cyber Liability Insurance" has become one of the best choices for entities storing and processing data of its users.

With Indian market getting increasingly competitive day-by-day, it becomes necessary for companies to focus on cyber security vis-a-vis cyber insurance.

In India, the insurance sector is regulated by "Insurance Regulatory and Development Authority (IRDAI)", an autonomous and statutory body constituted by Insurance Regulatory and Development Authority (IRDA) Act of 1999[39]. IRDAI conducted a study on cyber insurance

[35] Digital Personal Data Protection Act, S. 8(5).
[36] Digital Personal Data Protection Act, S. 8(6).
[37] Digital Personal Data Protection Act 2023, S. 10.
[38] Digital Personal Data Protection Act 2023, The Schedule.
[39] Insurance Regulatory and Development Authority of India (IRDAI), [Title of Document] (IRDAI, [1999]) <https://irdai.gov.in/document-detail?documentId=366291> accessed 14 July 2025.

market of India in 2021 by issuing a paper titled as "Guidance Document on Product Structure for Cyber Insurance[40]". There were certain notable observations that were made by the body: -

1. Out of the total cyber-crimes reported in the last decade, 80% of them had intention of "unlawful financial gain", also there is low consumer awareness among users about cyber fraud and therefore most of the instances go unreported.
2. Focus was also laid out on the "individual cyber insurance" and how it could provide financial security in the form of indemnity.
3. Following were the recommendations that were made-
    - Compulsory filing of FIR becomes a hassle for the claimant and an e-complaint filed before National Cyber Crime Reporting Portal can be considered for claims up to Rs. 5000.
    - Due diligence, care and diligence are required to maintain the claim before the insurer because any slight incident of negligence makes their claim unacceptable. This could be remedied by using specific terms in the insurance policy which doesn't leave any grey area.
    - Cyber Insurance coverage can be extended to cover cyber-attacks committed from outside India
    - Organize regular awareness initiatives to make cyber insurance accessible to the public.

DSCI also conducted a study and published a report titled "Cyber Insurance in India- mitigating risks amid changing regulations & uncertainties" in the year 2019, in this report DSCI highlighted various factors affecting and related to cyber insurance.

[40] Insurance Regulatory and Development Authority of India, IRDAI Circular on Cyber Security – Guidelines for Insurers (3 June 2024) <https://irdai.gov.in/document-detail?documentId=976463> accessed 11 July 2025.

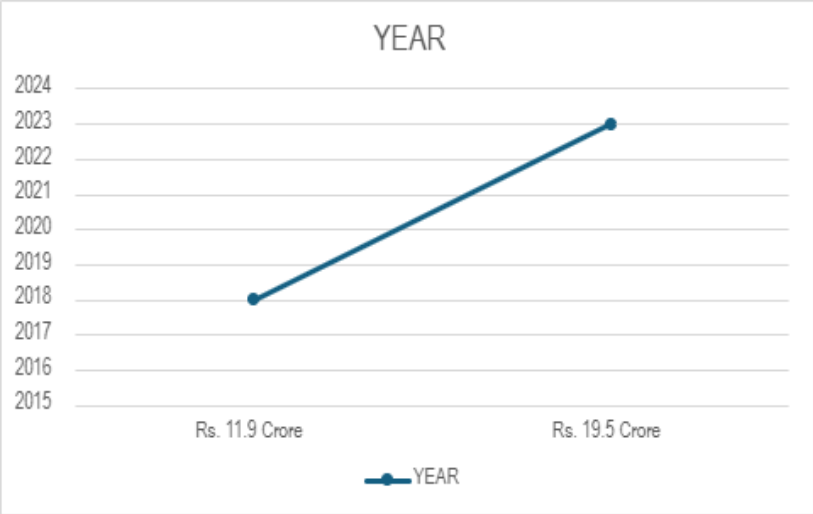


Figure IV: Graphical Representation of the rapid rise in average cost of data breach in India

According to this report, the average cost of data breach in India was around Rs. 11.9 Crore in 2018 which saw a spike of 8% from 2017 [41]. Bringing the contemporary record in context, according to the latest report of IBM titled "Cost of a Data Breach Report 2024[42]", the average cost of data breach in 2023 has reached already Rs. 19.5 Crore which is a 63% jump in just five years. This is the level of monetary impact (on average) of each data breach caused by cyber-attack, which has been exponentially rising.

Further, the report also highlighted that 350 cyber insurance policies were sold in India till 2018 which has reached a market share of USD 582.2 million in 2024[43] . The major reason behind Indian companies being driven towards cyber insurance is news of cyber-attack, while awareness/ educational initiatives has been of less effect in bringing people under insurance cover.

In India, the "First International Cyber Insurance Summit 2021" was held amid the Covid-19 pandemic, under the collaboration of GIC Re, Data Security Council of India (DSCI) and City of

[41] Data Security Council of India (DSCI), Cyber Insurance in India – Mitigating Risks Amid Changing Regulations & Uncertainties (Knowledge Resource, DSCI 2023 <https://www.dsci.in/resource/content/cyber-insurance-india> accessed 14 July 2025.

[42] IBM, 'IBM Report: Escalating Data Breach Disruption Pushes Average Cost of a Data Breach in India to All-Time High of INR 195 Million in 2024' (Newsroom IBM, 31 July 2024) <https://in.newsroom.ibm.com/2024-07-31-IBM-Report-Escalating-Data-Breach-Disruption-Pushes Average-Cost-of-a-Data-Breach-in-India-to-All-Time-High-of-INR-195-Million-in-2024> accessed 14 July 2025.

[43] IMARC Group, *India Cyber Insurance Market: Size, Growth, Trends, Share, Analysis, Report 2025–2033* (Market Research Report, IMARC Group 2025) <https://www.imarcgroup.com/india-cyber-insurance-market> accessed 14 July 2025.

London Corporation[44] where various stakeholders were invited and it was observed that "cyber education" and "cyber mitigation" are the two pillars of cyber security. Further, it was accepted that "cyber risk cannot be eliminated but mitigated".

Unfortunately, this was the only summit that took place in India concerning "cyber insurance" and since then no policy initiatives has been taken by the Government. Especially at a time when "AI" and "cloud computing" have taken over the internet, companies across various sectors including banking, health, IT etc. show apprehension and their lack of preparedness against the ever-evolving cyber threats.

The Way Forward

In India, the cyber insurance market is developing at a steady pace due to legislative developments taking place through IT Act and DPDP Act and due to the fear of cyber risks.

The awareness initiatives have tried to educate people about probable cyber-attacks that they may face if they do not take precautionary steps, but since the technology has been rapidly evolving with the coming up of AI and cloud computing- the doctrine of *"prevention is better than cure"* falls flat because every time the cyber-attack comes with a different face.

Big entities (having a decisive market share) started buying cyber insurance policies to transfer their risk and mitigate cyber risks. Most of the insurers in this case were either American or European, as Indian markets currently lack adequate infrastructure. The role of the Government has been minimal in promoting cyber insurance in India.

In India, a cyber insurance policy is limited to transferring of financial risk. Rather, the focus should be equally on prevention mechanisms as well. The Indian Insurers need to realize that an efficient cyber insurance mechanism should not only leave customer with financial stability but also takes regular cyber safety assessment.

In India, there is a lack of intellectual infrastructure which can guide the probable insurers towards a useful cyber insurance policy. Unless and until the nature of cyber risk is assessed, a cyber insurance policy cannot work efficiently. The Indian insurers currently lack a support system that

[44] Data Security Council of India (DSCI), *Cybersecurity Centre of Excellence (CCoE)* (DSCI, 2025) <https://www.dsci.in/content/cybersecurity-centre-excellence> accessed 14 July 2025.

is insured friendly. Such system can only be established when the Indian crowd becomes aware of cyber insurance policies. Initiatives need to be taken from the end of the Government and from the end of the insurers.

The awareness initiatives and adequate fund allocation for cyber insurance project shall bring the Indian crowd close to cyber insurance. While adequate guidance and support from the insurers shall build a trust of the people towards cyber insurance policies.

This will also include Government providing data and analytics regarding cyber space, setting up cyber-crime infrastructure for effective prevention and reporting of cyber-crimes, providing subsidy and incentives to the people to buy such policies.

Conclusion

The purpose of this research paper was to highlight the importance of cyber insurance as an appropriate mode of cyber resilience mechanism. This paper borrowed the relevancy of cyber insurance from the quantum of cyber incidents that our country is facing amid rapid advancement in technology.

Whenever we talk about cyber security, we are driven by this belief that prevention is an effective way towards cyber safety. I believe we are obsessed with this belief, and to ensure quality in our cyber security landscape we need to evolve in our decision-making. So, the priority should be preparation for cyber incidents and not mere prevention.

Cyber Insurance works on the "preparation strategy" and is a balanced approach towards achieving cyber security. In this paper, the author has tried to impart awareness about cyber insurance by defining its scope of operation along with the areas of its exclusion. A comparison has also been made of the working of cyber insurance in USA, Europe with that of India. Also, observations and recommendations have been made for making a better environment of cyber insurance in India.

The author started this paper with a hypothesis that "prevention alone is not an effective way towards cyber security", and after undergoing the research it is found that the hypothesis is proven right. Since, in the absence of cyber insurance, the data is at huge risk and therefore cyber insurance is the need of the hour.