# IMPACTS OF TECHNOLOGICAL ADVANCES ON INSURANCE SECTOR: A STUDY ON CYBER INSURANCE IN INDIA

Aditi Singh, B.A.LL.B., Alliance University

**ABSTRACT**

Societies all over the world have become increasingly dependent upon IT infrastructure and services. Due to the COVID-19 pandemic, everything has shifted from the traditional way of working to a more flexible and comfortable area of working, i.e. Internet or working remotely. This has led to an increase in cyberattacks, cyber threats that result in data breaches and other digital risks that pose significant financial and reputational consequences to organizations. In response to these growing threats, the demand for cyber insurance has increased. This rapid technological change has affected and presented unique challenges for the Insurance sector in India. Towards the protection from these risks, Cyber Insurance is considered as a strategic risk management instrument.

**Keywords:** Insurance, Law, Cyber, India

## INTRODUCTION

The increased dependency of modern society on digital services has resulted the companies significantly investing in administrative and regulatory countermeasures to prevent accidental and malicious cyberattacks or cybersecurity incidents. Nonetheless, the realizations and synchronicities of cyberattacks and cybersecurity incidents that cause severe impacts on companies & organizations, have made it quite evident that organizations cannot rely on their traditional risk mitigation measures. Cyber insurance has been available since the 1970s with a market growing with tech risks or errors, because of this many financial institutions' data breaches were the topmost issue. In the 1980's the first tech E&O policies were introduced that included cybersecurity insurance, particularly for financial institutions and blue-chip organizations.

During that time, cyber insurance was the stand-alone product that was filling or designed to fill the gap of traditional products in preventing breaches in the year 2000's. Following to years of 2000's, because of the Dotcom crash and the attack of 9/11, the interest and need for cyber insurance or security grew. There was a significant realization within the market that the technology or digital world did not necessarily fit within the traditional type of insurance covers/classes or insurance. As, organizations main concerns were the spreading of the virus, malware of different types and their legal liability towards the data breach. There was an important recognition that interruptions in their virtual events or business can cause substantial losses to business which unlikely were not covered by the traditional insurance policies and business policies as well. The growing cyber vulnerabilities did not instantly increase the demand for cyber insurance, the need for it grew in 2002, when the first data breach notification law was introduced in California, U.S.A. and other states followed that mandated the companies had to disclose immediately the breach of data to its customers, in writing and regulations with the authorities. The idea of cyber insurance was introduced by Dan Geer, who gave the relevance of the use of risk management, including internet insurance. He was the first to identify the importance and relevance of risk management in other fields, especially in the financial sector. Furthermore, there were many spokespersons, but the person who included this topic of cyber-insurance in academic discussions was Bruce Schneider.

The introduction of Cybersecurity laws/cyber insurance was seen in India in 2000, when the Information Technology Act, 2000 was passed. According to the report of digital security

firm, Gemalto, in 2018, India is the second highest country with the most data breaches in the world. Because of this, the importance of cyber-insurance is growing rapidly in India, as in the last five years, India's cyber-insurance market has tripled in size.

This paper will include the development of cyber insurance over time from when it was first introduced in the late 1990s through 2000. Cyber insurance development has certainly been affected by unforeseen events that we discuss in this paper. While it is hard to make generalizations about a market consisting of specific cyber insurance contracts, we do identify trends that have occurred which may reveal insights for the future.

## LITERATURE REVIEW

The historical context of cyber insurance, tracing its origins and growth alongside advancements in technology and changes in the cyber threat landscape. They examine various factors influencing the adoption of cyber insurance, including regulatory frameworks, market dynamics, and the evolving nature of cyber risks. Additionally, the paper discusses challenges and opportunities facing the cyber insurance industry, such as data breaches, underwriting complexities, and emerging trends in risk assessment. By synthesizing insights from existing literature, the authors offer valuable perspectives on the role of cyber insurance in mitigating cyber risks and enhancing cyber resilience for businesses and organizations in the digital age. (Ruperto P. Majuca). The growing threat posed by cyber-attacks and the challenges faced by insurance companies in underwriting cyber insurance policies. The paper discusses the need for innovative approaches to cyber risk management and highlights the importance of collaboration between insurers, policymakers, and cybersecurity experts. Through a comprehensive review of existing literature, Camillo provides insights into the changing dynamics of cyber insurance and its significance in addressing the complex challenges of cybersecurity in the digital age (Camillo, 2017). How advancements such as artificial intelligence, big data analytics, and blockchain are reshaping traditional insurance processes, from underwriting to claims management. The paper discusses the potential benefits of technology, such as improved risk assessment, operational efficiency, and enhanced customer experience. Additionally, the author addresses the challenges and risks associated with technological integration in insurance, including data privacy concerns and cybersecurity threats. Through a comprehensive literature review, the paper provides valuable insights into the evolving landscape of the insurance industry in the digital era (Mosleh, 2019). The authors

analyse how digitalization is reshaping the insurance value chain and influencing the insurability of risks. They explore the implications of technological advancements such as artificial intelligence, the Internet of Things (IoT), and data analytics on various aspects of insurance operations, including product development, distribution channels, underwriting, and claims processing. The paper provides valuable insights into the transformative effects of digitalization on the insurance industry (Martin Eling, 2017). The authors investigate the potential impact of cyber-insurance on network security. Through a literature review, they examine various perspectives on the efficacy of cyber-insurance as a tool for incentivizing organizations to enhance their cybersecurity measures. The paper critically evaluates the relationship between cyber insurance and network security, offering insights into the challenges and opportunities associated with using insurance mechanisms to mitigate cyber risks (Ranjan Pal, 2014). The author explores the role of cyber insurance in addressing corporate cyber insecurity. The author investigates how cyber insurance can incentivize organizations to invest in cybersecurity measures. The paper highlights the potential of cyber insurance as a mechanism for aligning incentives and reducing cyber risks (Miller, 2019). The author conducts an institutional analysis to examine the development of the cyber insurance industry. The author explores the institutional factors shaping the growth and dynamics of the cyber insurance market, providing insights into its evolution and prospects (Kshetri, 2020). Deloitte surveys in 2023 to explore the landscape of cyber insurance in India. The survey examines the current challenges and opportunities in the Indian cyber insurance market, providing insights into the strategies needed to navigate risks and capitalize on the opportunities presented by the digital economy (Deloitte, 2023).

## RESEARCH HYPOTHESIS

The advancement of technology has reshaped insurance law, particularly in the domain of cyber insurance, influencing coverage, regulation, and risk management strategies. This paper hypothesizes that as technology continues to evolve, cyber insurance will play an increasingly critical role in mitigating financial losses and promoting cyber resilience, necessitating ongoing adaptation of regulatory frameworks to address emerging cyber threats effectively.

## RESEARCH METHODOLOGY

This study is based on doctrinal research. To complete this work, secondary sources were used,

including statutes, articles, newspapers, debates, magazines, cases, research papers etc. These secondary sources were analysed systematically.

## 1. Evolution of Cyber Insurance

Cyber insurance has been available since the 1970s with a market growing with tech risks or errors, because of this many financial institutions' data breaches were the topmost issue. In 1980 the first tech E&O policies were introduced that included cybersecurity insurance, particularly for financial institutions and blue-chip organizations[1].

During that time, cyber insurance was the stand-alone product that was filling or designed to fill the gap of traditional products in preventing breaches in the year 2000's. Following to years of 2000's, because of the Dotcom crash and attack of 9/11, the interest and need for cyber insurance or security grew[2]. There was a significant realization within the market that the technology or digital world did not necessarily fit within the traditional type of insurance covers/classes or insurance. As, organizations main concerns were the spreading of the virus, malware of different types and their legal liability towards the data breach. There was an important recognition that interruptions in their virtual events or business can cause substantial losses to business which unlikely were not covered by the traditional insurance policies and business policies as well. The growing cyber vulnerabilities did not instantly increase the demand for cyber insurance, the need for it grew in 2002, when the first data breach notification law was introduced in California, U.S.A. and other states followed that mandated the companies had to disclose immediately the breach of data to its customers, in writing and regulations with the authorities.

At first cyber insurance policies did not cover and include both First-party and third-party coverage. It wasn't until the mid-2000s that these policies evolved because of cyber threats to add some first-party coverages to protect the organization as an individual and potential ips.

The idea of cyber insurance was introduced by Dan Geer, who gave the relevance of the use of risk management, including internet insurance. He was the first to identify the importance and relevance of risk management in other fields especially in the financial sector. Furthermore,

[1] Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, 53-63.
[2] Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, 53-63.

there were many spokespersons, but the person who included this topic of cyber-insurance in academic discussions was Bruce Schneider.[3]

In the late 1990s and early 2000s, the widespread adoption of the Internet and the subsequent increase in cybercrime marked a significant milestone in the evolution of cyber insurance. A surge in cyber insurance demand followed high-profile cyberattacks, such as the "ILOVEYOU" virus in 2000 and the Code Red worm in 2001.

### 1.1 Traditional insurance policies

Traditionally, companies or firms rely mostly on the insurance policies given by an insurance company which usually cover, (1) business personal insurance policies (to cover first-party losses); (2) business interruption policies; (3) commercial general liability (CGL) or umbrella liability insurance policies (to cover liability for damages to third parties); and (4) errors and omissions insurance (to cover the firm's officers). These traditional policies were designed to cover traditional losses such as fire, property, health, or other natural events. Since these policies were made before the born of the internet, therefore, insurance companies did not expressly cover internet-based losses, and because of that insurers pay heavy litigation charges in the courts to recover the amounts from the insurance companies.[4]

As an example, attacks on cyber properties may not result in any physical damage, since digital property doesn't necessarily have a physical form. The traditional policies do not guide what constitutes "tangible" property and "physical" damage, and consequently, many disputes have arisen between insurers and firms.

In Retails Systems, Inc. v. CNA Insurance Companies, 469 N.W.2d 735 [Minn. App. 1991], the court ruled that computer taps and data are tangible property under the CGL since the data had permanent value and was incorporated with the corporeal nature of the tape. Also, in American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc., Civ. 99-185 TUC ACM, 2000 WL 726789 (D. Ariz. April. 18, 2000), the Arizona court ruled that the loss of programming in a computer's RAM constituted physical loss or damage.[5]

[3] Ruperto P. Majuca, W. Y. (n.d.). The Evolution of Cyberinsurance.
[4] Ruperto P. Majuca, W. Y. (n.d.). The Evolution of Cyberinsurance.
[5] Ruperto P. Majuca, W. Y. (n.d.). The Evolution of Cyberinsurance.

Furthermore, most of the CGL policies do not provide worldwide coverage so covering attacks from international territory is difficult for the insurance companies, as it is evident that most cyber-attacks can be from anywhere in the world.

### 1.2 Increasing Risk & legislation compliance

In India, the major serious internet attacks have been seen since 2015, when attacks like Cosmos Bank Cyber Attack in Pune, 2016 debit card data breach, Aadhar data breach, etc been seen. On the other hand, worldwide, the need for cyber-security or cyber insurance was more evident and seen as necessary, especially after the attack of 9/11 on September 11th, 2001. There had been many cyber risks before the attack of 9/11 but things started to look differently after the attack. The three most serious cyber-attacks that happened around the attack of 9/11 were Code Red in July 2001, Nimda in September 2001, and Klez in October 2001. There were major DoS attacks against some big US corporations that affected 5 out of 10 most popular internet websites and led to the slowing down of the entire internet.

Furthermore, hackers have targeted authentication systems, computer intrusions, web defacement, phishing, and identity theft. The majority of businesses and government agencies have detected security breaches, with 75% of these businesses suffering financial losses as a result. There are 34% of organizations that admit they don't know if their systems are compromised, and 33% that aren't able to react. Despite this, crackers have attacked not only businesses, but also key government agencies like the Senate, the Federal Bureau of Investigation (FBI), the National Aeronautics and Space Administration (NASA), and the Department of Defense (DoD).[6] A virus called the Love Bug (2000) affected 20 countries and 45 million users, causing the loss of $8.75 billion in productivity and damage to software. It is more evident now that, the cyber security risks have increased since 2000-2003 and financial institutions and firms need legislation and coverage regarding the same.

In the recent survey done by Deloitte in October 2023, wherein it was cited that India is expected to face a lot of cyber-attacks because it's trying to use technology for growth, like using cloud, metaverse, and AI, and making its public systems more digital Bharat. This has made it a good target for cybercriminals.[7] According to the FBI, India is fourth on the list

[6] Ruperto P. Majuca, W. Y. (n.d.). The Evolution of Cyberinsurance.
[7] Deloitte. (2023). *Cyber insurance in India: Navigating risks and opportunities in a digital economy.* Deloitte Survey Report.

of countries with the most cybercrime victims. The Computer Emergency Response Team (CERT) of India says India had 1.39 million cybersecurity problems in 2022. Since September 2022, India has had around 1,787 cyberattacks every week, which is more than the global average of 983 attacks per week[8].

There are other examples also of cyber-attacks in India in sectors like Pharma, Healthcare, Government, Infrastructure etc. A report published by the CyberPeace Foundation and Autobot Infosec revealed that the Indian healthcare sector experienced 1.9 million cyberattacks until November 2022. In November 2022, one of India's largest companies was hacked. In the same month, a state-run oil producer, an Indian airline operator (SpiceJet), and a leading power generation company (Tata Power) were also attacked by cyber attackers. Private information of another public-listed Indian pharmaceutical corporation named Aarti Drugs Ltd. was disclosed on a dark web forum[9].

## 2. Introduction to Technological Advances in Insurance Law

After the break of Covid-19, the market has been very hostile which has introduced rapid changes in the technological environment, which affects all aspects of our lives and introduces us to more smart solutions and new platforms with more developed channels in the insurance industry that can improve the sector profoundly. Due to fast-changing technological advancements, the insurance industry is facing serious dilemmas and witnessing serious challenges regarding the same. These technological innovations have introduced the Internet of Things (IoT), Blockchain and Artificial Intelligence (AI).

In the recent past, radical technological advancement has increased the virtue of new technologies because of which another macro trend has revolutionized the market globally. The new technologies, like, applications, smart devices, and big data have increased the fluency and communications between people, through social media platforms, and are transforming the ways and methods of innovations, which has changed the insurance business and has increased the new ways and distribution channels in the insurance business.

[8] Lall, S. (2023, December 10). *The Economic Times*. Retrieved from Economictimes.timesindia: https://bfsi.economictimes.indiatimes.com/blog/cyber-insurance-an-evolving-story/105867676
[9] Deloitte. (2023). *Cyber insurance in India: Navigating risks and opportunities in a digital economy.* Deloitte Survey Report.

Technology has enabled the insurers to access large databases, because of which their risk exposures have increased, which were not covered in the past. For example in the business of Ridesharing, underwriters can accurately predict and measure the risk associated with each booking, and they can provide coverage for the same. Moreover, if we see the large picture with access to this large database, insurance companies have gained the opportunity to explore new distribution channels through giant internet companies, as Google, Facebook, Apple, and Amazon, and online shops and payment apps like Flipkart, Amazon, Phonepe, CRED etc.[10] Through these partnerships, insurance companies have the opportunity to access to a large pool of data of users, and through which they can sell their insurance products to huge customer base and can introduce new marketing strategies and can diversify their distribution methods.

As technology is changing and taking new turns every day, some market commenters anticipate that the traditional insurance business will soon fade out of business and will face the same fate as "Kodak" the company that failed to anticipate and adapt the future trends and declared bankrupt in 2012. However, most of the insurers also feel that technology is transformative and they have time to adjust to the technological advancement and become more customer-centric and can change their distributive methods.[11]

### 2.1 Development of technology in the insurance industry

In recent history the world has experienced two financial crises; the first one, occurred in the 1990s with the so-called IT and technology bubble, and, the second one was for the burst of the property/housing bubble that occurred between 2007 and 2008[12].

There are theories wherein some say that the insurance industry was influenced by technology because of the 1990s Dot Com bubble, wherein Investors poured lots of money into these companies, hoping they would make big profits. The bubble grew as more dot-coms went public, with their stock prices soaring. However, many of these companies didn't make much money and had shaky business plans. Eventually, the bubble burst in the early 2000s, causing stock prices to go down and many dot-coms to go out of business. It was a tough lesson for

[10] Mosleh, N. (2019, February ). Impact of Technology on Insurance Industry. *Impact of Technology on Insurance Industry*, pp. 2-28.
[11] Martin Eling, M. L. (2017). The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks . *The Geneva Papers on Risk and Insurance*.
[12] Mosleh, N. (2019, February ). Impact of Technology on Insurance Industry. *Impact of Technology on Insurance Industry*, pp. 2-28.

investors, showing that not all new technology companies would be successful and that investing in them could be a risky chance. This has led to significant losses in the stock market business and capital started to dry up, wherein companies worth millions of assets became insolvent in such a short time by the year 2001, many Dot-Com companies were closed forever and few survived, like Amazon & Google.

Due to the positive impact of the 1990s bubble, many companies got the opportunity to understand the risks associated with technological innovations and how they can majorly affect business operations, and this enabled the insurance companies to deeply understand their market & customer needs and to design their products accordingly.

### 2.3 Impact of technology on Distributive methods

Because of radical technological advancements, the insurance industry is facing new challenges and trends especially Tech developments and their impact on sales. The way insurers and customers interact has completely changed. Now, as insurance companies have access to substantial data, they can understand their customers' needs very accurately. Thus, the use of digital technology has not only changed the distributive channels but is completely a new way of doing business.

There are new ways to sell insurance apart from using agents and brokers. These methods are becoming popular, especially for start-ups, because they are cheaper. Unlike agents and brokers, start-ups don't have to spend a lot on distribution channels. This is good news for customers because it means they can get insurance at lower prices.

The rise of digital technology is changing how insurance companies grow and operate. It's also shaking up the ways insurance policies are sold. Digital platforms are changing how companies talk to customers, work with suppliers, and manage employees.[13]

Because of the change in the insurance industry to Phytical (Physical & digital) Model[14], Insurance companies are making significant changes to how they do things with the help of

[13] Mosleh, N. (2019, February ). Impact of Technology on Insurance Industry. *Impact of Technology on Insurance Industry*, pp. 2-28.
[14] Singhel, T. (2023, August 20). *The Economic Times*. Retrieved from economictimes.indiatimes: https://economictimes.indiatimes.com/markets/stocks/news/how-ai-blockchain-technology-are-taking-indias-insurance-industry-to-next-level/articleshow/102872373.cms?from=mdr

technology. Processes like issuing policies, handling claims, and doing medical checks used to involve a lot of paperwork. Now, they're using digital tools to make these processes smoother & faster for customers and to make things more efficient.

Technologies such as machine learning, AI, automation, and data analytics are helping insurance companies with this. For example, insurance companies are using AI-powered chatbots and virtual assistants to give customers a personalized look and help with things like filing claims, renewing policies, and dealing with and resolving their problems in the fastest and easiest way possible[15].

They're also using AI and machine learning to make important decisions about things like pricing policies. This allows them to offer better products that match each customer's needs and risks.

**Problems in the development of cyber-insurance**

There is a basic understanding while determining the cyber-insurance business, like Why companies that don't want to spend much on cybersecurity want to get more cyber insurance coverage in the future. Could it be that they're looking to transfer their risks to insurance companies instead of strengthening their online security? Are they concerned that new data privacy laws might soon require them to have cyber insurance?

Even though they know cyber insurance is important, companies with little coverage are still thinking about whether they should get more benefits. Is it because they're not sure if insurance will be worth it for them?[16]

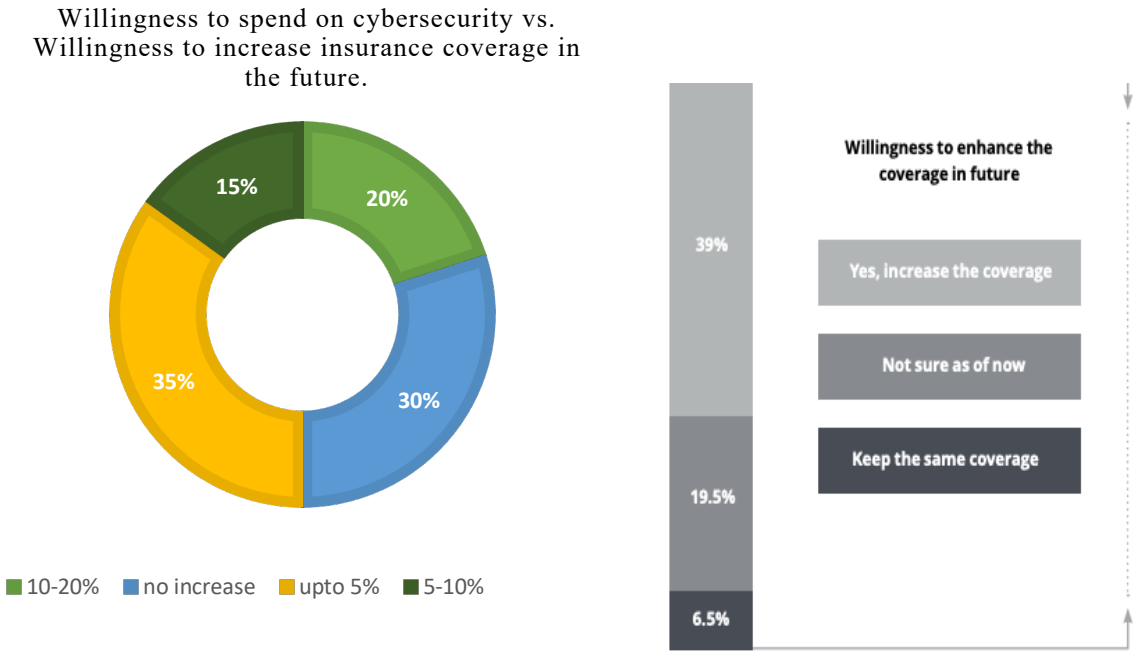
Dissatisfaction is the major setback in the growth of the cyber-insurance business in India. Because companies see cyber-insurance as their additional burden because they are already spending a heavy amount on strengthening their digital infrastructure. Thus, purchasing insurance will demotivate the company to spend or maintain its cyber-security infrastructure

[15] Singhel, T. (2023, August 20). *The Economic Times*. Retrieved from economictimes.indiatimes: https://economictimes.indiatimes.com/markets/stocks/news/how-ai-blockchain-technology-are-taking-indias-insurance-industry-to-next-level/articleshow/102872373.cms?from=mdr

[16] Deloitte. (2023). *Cyber insurance in India: Navigating risks and opportunities in a digital economy.* Deloitte Survey Report.

strong. Moreover, companies feel that the hackers target particularly that companies more which have cyber-insurance and eventually that will increase the insurer's cost.

Another problem is finding out that, the taxes when companies get money from cyber insurance claims. It's not clear whether the money they get from Insurance Co. should be taxed or not. Also, if an insurer pays ransom money, can they get a tax deduction for the same? There is no clarity till now on these aspects.




The represented data was presented in the Deloitte Research Survey of 2023, wherein it is evident that a large proportion of the people has lesser interest towards increasing the budget for cyber-security, but on the other hand some have already invested in cyber insurance have the willingness to have more coverage, but without wanting to invest more in digital security infrastructure[17]

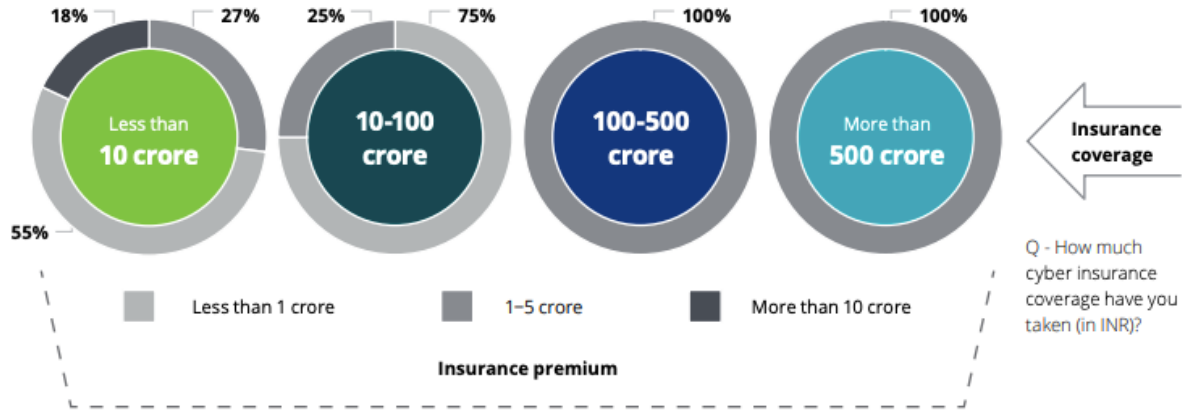
As cyber risks are constantly evolving, therefore buyers of the policies have very limited clarity towards the incidents that will be covered by the cyber insurance. There is quite an unfamiliarity with the procedures and claims settlement and thresholds that are ambiguous and resolutions that cannot be resolved efficiently by the insurance companies. Because of these unresolved questions companies take insurance policies based on the company's benchmark

[17] Deloitte. (2023). *Cyber insurance in India: Navigating risks and opportunities in a digital economy.* Deloitte Survey Report.

(just to buy policies higher than their competitors in the market) and do not understand the true value or the measurement of cyber risks involved as per their company's infrastructure.[18]

Another major problem in the case of cyber insurance policies is to determine the accurate risk that can be done to a policyholder, as the internet is the spider web, wherein if company A's digital infrastructure is attacked or compromised, then it can affect the other companies infrastructure also, and that becomes a problem in quantum of pay-outs in case of attacks. For example, if there is damage to a physical property (say vehicle) or a death of a person due to an accident or natural death, it is still estimable for the coverage issue. However, the clear visibility of the risks of cyber-attacks is not measurable and is unpredictable. Because of this, the policyholder's profile becomes inconsistent[19]

**Fig. 2 The insurance premium paid and the insurance coverage**




The represented data was presented in the Deloitte Research Survey of 2023, where the survey has clearly stated that roughly around 40% of the companies, firms or policyholders have a strong gap and have lacked in payment of premiums and their policy coverage issue. A majority paid a higher premium for the insurance coverage they received and most of these firms belonged to the consumer sector[20].

Another major problem that arises in the case of cyber insurance are crisis during any geopolitical war, wherein cyber-security becomes very vulnerable and more prone to cyber-

[18] Deloitte. (2023). *Cyber insurance in India: Navigating risks and opportunities in a digital economy.* Deloitte Survey Report.
[19] *Supra*
[20] *Supra*

security problems. The most common example is Terrorism, because of which cyber Insurance companies are still unaware of how to give coverage for these kinds of situations. One famous case involved an American snacking giant that bought cyber insurance and was denied payment by a Swiss insurance company. 'NotPetya' ransomware attacks were not covered by the insurance company's policy because they were considered "acts of war".[21]

**Cyber Security laws in India**

The report indicates that the current Indian cyber insurance market is valued at US$ 50–60 million, maintaining a steady 27–30 per cent CAGR in the past three years. This growth is expected to continue for the next 3–5 years, driven by an increased awareness of the need for cyber insurance[22]. This India has been quite evident and proactive towards making the laws and guidelines to prevent more cyber-attacks ratio in India. But the basic problem is that technology is taking a new turn every day, and cyber-attacks are also emerging of different kinds, and Indian cyber-security is still outdated and unclarified statutes. To maintain cyber-security standards, India must make more stringent laws of cyber & data protection laws.

A SLP was filed in 2021, wherein the Supreme Court of India ruled that cyber-attacks and data thefts are a crime under the Information Technology Act (IT Act) of 2000 and the Indian Penal Code (IPC). It was held that a more modern and renewed IT Act of 2000 is the main regulation against cybercrime as of today[23]

Perse, four major statutes govern the cyber-security laws in India, which are:

1. Information Technology Act, 2000

2. Indian Penal Code, 1860

3. Digital Personal Data Protection Act, 2023

[21] Deloitte. (2023). *Cyber insurance in India: Navigating risks and opportunities in a digital economy.* Deloitte Survey Report.
[22] Deloitte. (2023). *Cyber insurance in India: Navigating risks and opportunities in a digital economy.* Deloitte Survey Report.
[23] Chin, K. (2024, January 18). *upguard*. Retrieved from upguard.com: https://www.upguard.com/blog/cybersecurity-regulations-india#:~:text=The%20IT%20Act%20of%202000,protection%20policies%2C%20and%20govern%20cybercrime.

4. National Cyber Security Policy, 2013

Cybersecurity laws in India are essential for protecting individuals, businesses, and the government online. As a result of these laws, sensitive information is safeguarded, cybercrimes are prevented, and digital technology is used securely.

1. The IT Act is the primary law governing cyber security in India. It defines cybercrimes such as hacking, identity theft, and spreading viruses. The Act also provides legal recognition for electronic records and digital signatures, making online transactions secure.

2. Certain sections of the IPC deal with cybercrimes. For example, Section 66C deals with identity theft, while Section 66D addresses cheating by personation using computer resources.

3. **National Cyber Security Policy, 2013** wherein the government formulated this policy to protect national interests in cyberspace and enhance the security posture of the country. It aims to build a secure and resilient cyber ecosystem by promoting cybersecurity awareness, creating mechanisms for incident response, and fostering international cooperation.

4. **Data Protection Laws by the Indian Government have not passed a comprehensive Data Protection Law as of yet, but certain regulations are in place to ensure that personal data is protected.** For instance, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 prescribe standards for protecting sensitive personal data collected by entities[24].

5. CERT-In is the nodal agency responsible for coordinating responses to cyber security incidents in India. It provides incident prevention, detection, and response services to safeguard the country's cyberspace.

6. The Reserve Bank of India (RBI) issues guidelines and regulations to ensure the security of online banking and financial transactions. These regulations mandate banks to implement robust cyber security measures to protect customer data and prevent financial fraud. For example: KYC methods used by the Indian Government and RBI.

[24] Deloitte. (2023). *Cyber insurance in India: Navigating risks and opportunities in a digital economy.* Deloitte Survey Report.

7. Certain industries, such as healthcare and telecommunications, have specific regulations governing cyber security. For example, the Health Insurance Portability and Accountability Act (HIPAA) in healthcare and the Telecom Regulatory Authority of India (TRAI) regulations for telecommunications.

8. Cyber Regulations Appellate Tribunal (CRAT), Under the IT Act, 2000, Section 62, the Central Government of India created the Cyber Regulations Appellate Tribunal (CRAT) as a chief governing body and authority for fact-finding, receiving cyber evidence, and examining witnesses[25].

The Indian government has emphasised a lot on the security of the digital sector and to regulate that the Malhotra Committee had introduced Insurance Regulatory and Development Authority of India (IRDAI), IRDAI, is called Insurance watchdog of India, plays a significant role in maintaining insurance companies secure from cyber-attacks. It sets & makes rules and guidelines to make sure that these companies protect people's sensitive information, like their policies & sensitive details. IRDAI's guidelines help insurance companies understand how to assess and manage cyber risks, and what to do if there's a cyber-attack.

IRDAI also help insurance companies to provide cyber insurance to grow businesses and help individuals protect themselves from cybercrimes. It keeps an eye on insurance companies to make sure they are following to these rules and guidelines. If a company does violate the cyber security rules, IRDAI takes strict actions to make sure they are not in breach.

Overall, IRDAI works to make sure insurance companies are prepared to handle cyber-attacks and keep every individual data protected.

Furthermore, as the media of any country is a very important part of the every country's economy, hence, Telecom Regulatory Authority of India (TRAI) regulates the telecom industry of India and ensures that the telecom service providers must adhere to cyber security measures. They set rules and guidelines for cyber security, issue directives to telecom operators, and collaborate with stakeholders to prevent cyber-attacks.

[25] Chin, K. (2024, january 18). *upguard*. Retrieved from upguard.com: https://www.upguard.com/blog/cybersecurity-regulations-india#:~:text=The%20IT%20Act%20of%202000,protection%20policies%2C%20and%20govern%20cybercrime.

Moreover, the Department of Telecommunications (DoT) make policies and regulations for the telecommunications sector of India, including cyber security. It works closely with TRAI to develop and implement cyber security measures and laws, issuing guidelines and regulations to telecom operators regarding cyber security requirements, data protection, and reports of digital attacks.

Together, TRAI and DoT play vital roles in shaping cyber security laws in India's telecom sector more efficiently. They focus on safeguarding critical infrastructure, protecting consumer data, and ensuring the resilience of telecommunications networks against cyber threats through regulations, collaboration, and awareness initiatives.

**Trends and Future Directions in Cyber Insurance**

After the Pandemic of 2020, cyber security and awareness have been the main concerns of every economy in the globe. As the paper has deliberately discussed the detailed impacts, advancements and problems in the cyber-insurance business. As there are many setbacks or roadblocks in the growth of cyber Insurance, there are only three major reasons why cyber insurance can grow in India exponentially.

1. As the digital infrastructure of the firms or institutions grows, the threat to their cyber infrastructure will become rare. Because of this the firms will have a better understanding towards their future risks and can increase the willingness to secure and enhance their security safety[26].

2. It is a must for the government to make more strict cyber-insurance policies. Which will mandate the firms to opt for cyber-insurance policies as a guideline mandated by the government. The government will also become the biggest consumer itself, because as everything is digitalized today, the government system has the sensitive information of every citizen of the country, and because of this the private firms will have a positive effect. Collaborations with the government will mandate that private firms necessarily opt for cyber-insurance.

[26] Deloitte. (2023). *Cyber insurance in India: Navigating risks and opportunities in a digital economy.* Deloitte Survey Report.

3. Many new types of companies, like technology firms and multinational corporations (MNCs), are now getting into the cyber insurance business. This is making the market more competitive. But with these new players coming in, there are also opportunities for traditional insurance sellers to improve their game. They can do this by investing in technology and teaming up with innovative tech companies, cloud service providers, and start-ups that specialize in big data. Technology companies have a lot of data and money that insurance companies don't have. On the other hand, insurance companies know a lot about assessing risk. If they work together, they can gather more security data and better understand the cyber risks faced by their customers. With this knowledge, they can create cyber insurance policies that fit the needs of their customers better[27].

The Master Directions of IT outsourcing for banks, financial institutions, and other regulated businesses were released by the RBI on 10 April 2023. The directive stipulates that financial institutions must ensure that cyber incidents are reported to the RBI within six hours of the incident. One of the essentials of cyber insurance policies is to notify insurers of a cyberattack within a certain timeframe, helping in faster and more transparent claim processing. Under the new directions, financial institutions can avoid any coverage disputes that could arise from delayed reporting[28]. Hereafter, the government plays a crucial role in the future growth of the cyber-insurance sector in India. There are particularly four areas wherein efforts or push is required from the government side,

1. The government can encourage or mandate the sharing of information about cyber threats and attacks among insurance companies, cybersecurity experts, and other organizations. This sharing of information can help the insurers to understand associated risks better and create policies that meet the needs of their customers. The government can promote this by creating platforms or sites for sharing information and providing appropriate incentives for collaboration.

2. The government must create clear rules and guidelines for cyber insurance. These rules can cover what cyber insurance policies should include, how much they should cost per individual, and how claims should be handled appropriately. When the law is clear,

[27] Deloitte. (2023). *Cyber insurance in India: Navigating risks and opportunities in a digital economy.* Deloitte Survey Report.
[28] Lall, S. (2023, December 10). *The Economic Times*. Retrieved from Economictimes.timesindia: https://bfsi.economictimes.indiatimes.com/blog/cyber-insurance-an-evolving-story/105867676

insurance companies can feel confident about selling cyber insurance, and customers can trust the insurer that they're getting the right coverage.

3. The prompt implementation of the Digital Personal Data Protection (DPDP) Act 2023 is need of the hour for the growth of cyber insurance in India. The act establishes clear rules for how personal data should be collected, stored, protected, and used by businesses and organizations. By protecting personal data more efficiently, the Act will reduce the risk of data breaches and digital-attacks, making it more easier for insurance companies to overlook and underwrite cyber insurance policies. Additionally, the act will increase trust between consumers, encouraging them to invest in cyber insurance to safeguard their digital infrastructure. The implementation of the DPDP Act will create a more secure & efficient digital environment, driving the demand for cyber insurance and promoting the growth of the cyber insurance market in India.

4. Establishing a dedicated adjudicatory system for online civil and criminal offences is essential for the growth of cyber insurance in India. This dedicated system would handle all legal disputes related to cybercrimes and data breaches, providing timely and effective resolution for both individuals and businesses. By streamlining the legal process and ensuring fair justice, the adjudicatory system would increase the overall cybersecurity landscape, reducing the frequency and severity of cyber incidents. Insurers would be more willing to offer cyber insurance policies knowing that legal recourse is available in case of a cyber-attack. Moreover, a specialized system would increase confidence among policyholders, encouraging greater adoption of cyber insurance to mitigate financial losses resulting from cybercrimes. Ultimately, the establishment of such a system would contribute to the development and expansion of the cyber insurance market in India.

## Summary

Cyber insurance is an important tool for Internet security especially at two levels, first, it provides economic incentives to the firms, individuals and insurers to manage their risks for profits, second, by cyber-insurance, there is more alignment towards social welfare.

We conclude that cyber insurance is making the Internet a safer environment because cyber insurers require businesses to minimize losses using economic incentives and individuals/organizations are increasingly seeing cyber insurance in their self-interest.

Insurers can make partnerships & collaborations of knowledge about risks, identify system-wide vulnerabilities, demand that the insured undergo prequalification audits, and adopt proactive strategies to prevent cyber-attacks. This is similar to what has happened in other industries where insurance increased safety in fire prevention, aviation, boiler and elevators.

In addition to compliance with legislation for protecting digital infrastructure, government subsidies are an additional option for encouraging firms to purchase cyber insurance following IRDAI model regulations and guidelines for such areas as accident and health insurance, and the intervention of the government for such areas as floods and nuclear power plant accidents.

Unfortunately, changes in risk management actions often require events of great magnitude. We have already mentioned 9/11 in this paper as one such event and other events like the 2016 Debit card hacks, Aadhar information hack, Data breach of many pharma companies and recently of an Airline. Unfortunately, it may take an Internet event of similar magnitude before cyber insurance increases its demand to higher levels but this is not a question of “if” but “when”.

## REFERENCES

Ruperto P. Majuca, W. Y. (n.d.). The Evolution of Cyberinsurance.

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, 53-63.

Mosleh, N. (2019, February ). Impact of Technology on Insurance Industry. *Impact of Technology on Insurance Industry*, pp. 2-28.

Martin Eling, M. L. (2017). The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks . *The Geneva Papers on Risk and Insurance*.

Ranjan Pal, L. G. (2014). Will Cyber-Insurance Improve Network Security? *IEEE Conference on Computer Communications* (pp. 235- 243). IEEE Conference on Computer Communications.

Miller, L. (2019). Cyber Insurance An Incentive Alignment Solution to Corporate Cyber-Insecurity. *Journal of Law & Cyber Warfare*, 147-182.

Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. *Elsevier Ltd*.

Deloitte. (2023). *Cyber insurance in India: Navigating risks and opportunities in a digital economy.* Deloitte Survey Report .

Lall, S. (2023, December 10). *The Economic Times*. Retrieved from Economictimes.timesindia: https://bfsi.economictimes.indiatimes.com/blog/cyber-insurance-an-evolving-story/105867676

Singhel, T. (2023, August 20). *The Economic Times*. Retrieved from economictimes.indiatimes: https://economictimes.indiatimes.com/markets/stocks/news/how-ai-blockchain-technology-are-taking-indias-insurance-industry-to-next-level/articleshow/102872373.cms?from=mdr

Chin, K. (2024, january 18). *upguard*. Retrieved from upguard.com: https://www.upguard.com/blog/cybersecurity-regulations-india#:~:text=The%20IT%20Act%20of%202000,protection%20policies%2C%20and%20govern%20cybercrime.

India, G. o. (2024, March 20). *Ministry of Electronics & Information Technology.* Retrieved from meity.gov: https://www.meity.gov.in/content/cyber-laws

Christian Biener, M. E. (2014). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice, 40*(1), 131-158.

Jayendra Kumar, S. M. (2016). Cyber Risk Insurance-An Indian Perspective. *International Journal of Advanced Research, 4*(7), 1270-1278.

Sood, G. (2014). Comparative Analysis of Cyber Privacy Law in India and in the United States of America. *law and politics, 12*(2), 129-135.

KPMG. (2015). *Cybercrime survey report 2015.* KPMG.com/in.