Certificate by the Mentor / Guide

CERTIFICATE

This is to certify that the Research Project entitled "CYBER Insurance**"** submitted by **Mr. Malpura Mohd Azharuddin Mohd Rafiq**, Seat No 8163020, for the partial fulfillment of **M.Sc. (Information Technology) Semester III** is a record of his independent work carried out under my guidance and supervision. To the best of my knowledge, this project work is original and has not been submitted for any other degree or examination.

Date:_____

Place: _____

Guide/Mentor:_____

Designation:_____

Department:_____

College: _____

Appendix III

Student's Declaration

I, Ms. Malpura Mohd Azharuddin Mohd Rafiq Student of University Of Mumbai College/Institute/ Department studying in MSC IT SEM 3, hereby declare that I have completed the Research project entitled CYBER INSURANCE during the academic year 2025-2026.

The report work is original and the information/data included in the report is true emerging from the primary and/ secondary data gathered and analyzed as part of this project. Due credit is extended on the work of Literature/Secondary Survey by endorsing it in the Bibliography as per prescribed format.

Signature of the Student with Date

Malpura Mohd Azharuddin Mohd Rafiq

Name of Student

ACKNOWLEDGEMENT

I take this opportunity to express my sincere gratitude to Shubhangi Ingole, my project guide, for her valuable guidance, encouragement, and continuous support throughout the completion of this research project.

I am thankful to University Of Mumbai **College**, the Head of the Department, and all faculty members of the **Department of Information Technology** for providing the necessary facilities and academic support.

I also extend my heartfelt thanks to my parents, friends, and classmates for their cooperation, motivation, and moral support during the course of this project.

Date:_____

Place: _____

Malpura Mohd Azharuddin Malpura

(Name of the Student)

Appendix I

Project Report

CYBER INSURANCE

Malpura Mohd Azharuddin Mohd Rafiq

M. Sc. (Information Technology) Part – II Semester III

M. Sc. (Information Technology)

Under the Guidance of

Shubhangi Ingole

Centre for Distance and Online Education (CDOE), Dr. Shankar Dayal Sharma Bhavan ,University of Mumbai,Vidya Nagari, Kalina, Santacruz East, Mumbai, Maharashtra 400098.

Academic Year – 2025-26

Appendix II

Centre for Distance and Online Education (CDOE), Dr. Shankar Dayal Sharma Bhavan ,University of Mumbai,Vidya Nagari, Kalina, Santacruz East, Mumbai, Maharashtra 400098.

Certificate

I hereby certify that Mr. Malpura Mohd Azharudin Mohd Rafiq, Student of University Of Mumbai College/Institute/ Department studying in M. Sc. (Information Technology) Part – II Semester III , has completed a project titled Cyber Insurance for the academic year 2025-2026. To the best of my knowledge the work of the student is original and the information included in the project is correct.

Name and Signature of
Research Project Guide

Name and Signature of
HOD

Name and Signature of
HOD/Principal/Director

Appendix IV

Student Feedback on Research Project

(To be filled by Students after Project completion)

Student Name:

Seat No. /Roll No.:

Email:

Department:

Name of the Mentor:

Title of Research Project:

Brief description of Project work carried out:

Year of completion of Research Project:

Was your project work experience related to your major area of study?

- Yes, to a large degree
- Yes, to a slight degree
- No, not related at all

Indicate the degree to which you agree or disagree with the following statements.

This experience has:	**Strongly Agree**	**Agree**	**No opinion**	**Disagree**	**Strongly Disagree**
Given me the opportunity to explore a career field					
Allowed me to apply classroom theory to practice					
Helped me develop my decision-making and problem-solving skills					
Expanded my knowledge about the work world before permanent employment					
Helped me develop my written and oral communication skills					
Provided a chance to use leadership skills (influence others, develop ideas with others, stimulate decision-making and action)					
Expanded my sensitivity to the ethical					

implications of the work involved					
Made it possible for me to be more confident in new situations					
Given me a chance to improve my interpersonal skills					
Helped me learn to handle responsibility and use my time wisely					
Helped me discover new aspects of myself that I didn't know existed before					
Helped me develop new interests and abilities					
Helped me clarify my career goals					
Allowed me to acquire information and/ or use equipment not available at my Institute					
Allowed me to realize socio-economic/environmental issues.					

● In the Institute Research Project, faculty members are expected to be mentors for students. Do you feel that your faculty mentor served such a function? Why or why not?

● How well were you able to accomplish the initial goals, tasks and new skills that were set down in your learning contract? In what ways were you able to take a new direction or expand beyond your contract? Why were some goals not accomplished adequately?

● In what areas did you most develop and improve?

● What has been the most significant accomplishment or satisfying moment of your Research Project?

● What did you dislike about the Research Project?

● Considering your overall experience, how would you rate this Research Project? (Circle one). –

Satisfactory/ Good/ Excellent

● Give suggestions as to how your research project experience could have been improved. (Could you have handled added responsibility? Would you have liked more discussions with your professor concerning your project work? Was closer supervision needed? Was more of an orientation required?)

Signature of Student
Name
Date:

Cyber Insurance

Chapter 1: Introduction

1.1 Background

The economic development of the country is possible when the nation takes the responsibility to perform and accountability to check the functions performed by it in a responsible manner.
Digitalization means the process of integration of converting any information in e-format with the help of developed technologies. It changes the business model along with the digital technologies. In this era of digitalization there is a possibility of higher level of transparency because of digital economy. But along with the benefits of digitalization, there is a possibility of cyber risk. When the digital data is accessed by any unauthorized source with the objective of making harm to the individual, group or any company directly or indirectly, physically or mentally by using any modern telecommunication network it becomes cyber- crime. Nation's financial health and security can badly affected by it. So for the purpose of cyber security information technology act has been passed in the year 2000. The cyber laws are there as a mechanism to give punishment to the person who made a cyber-crime.
Cyber insurance is a mechanism which secures the victim of cyber-crime by mitigating and providing the coverage against the losses arising out of cyber risk or cyber insecurity or cyber-crime. IT Act 2000 provides security against cyber-crime by punishing a criminal and IRDA provides mechanism for coverage of loss by cyber insurance.
This paper will helps to understand the role of cyber insurance and awareness of it in the era of digital economy among the participants. This is a fundamental research along with the secondary data sources. I am doing this research to create an awareness regarding cyber insurance in the present scenario.

In the post-Covid era, the proliferation of digital technologies has led to an unprecedented rise in cyber threats worldwide. India, with its ambitious Digital India initiative, has witnessed exponential growth in digital transactions, cloud computing, and artificial intelligence-driven business operations. However, this progress has been accompanied by a surge in cybercrimes, making cyber insurance an indispensable tool for risk mitigation. Cyber insurance provides financial protection against losses stemming from cyber incidents, including data breaches, system disruptions, and third-party liabilities. Despite its significance, the legal framework governing cyber insurance in India remains fragmented, necessitating comprehensive legislative and regulatory reforms.

1.2 Problem Statement

As cyber threats become more dynamic and unpredictable, its more struggle to maintain effectiveness. Cyber threats are constantly changing, with new attack vectors and malware emerging regularly. This makes it challenging for insurers to accurately predict future losses and set appropriate premiums. Unlike traditional insurance, there isn't a long history of cyber incidents to analyze and use for actuarial modeling. Cyberattacks can spread rapidly through interconnected systems, leading to large, correlated losses that are difficult to predict and model. Ransomware attacks are a major concern for cyber insurers, as they can cause significant financial losses and operational disruptions. Attacks on supply chains can also lead to

widespread losses, as a compromise in one organization can affect its customers and partners. Cyber insurance can be expensive, particularly for small and medium-sized businesses. Some businesses may not be fully aware of the risks they face or the benefits of cyber insurance. Some policies may not cover certain types of losses, such as reputational damage or loss of future revenue, leaving businesses vulnerable.

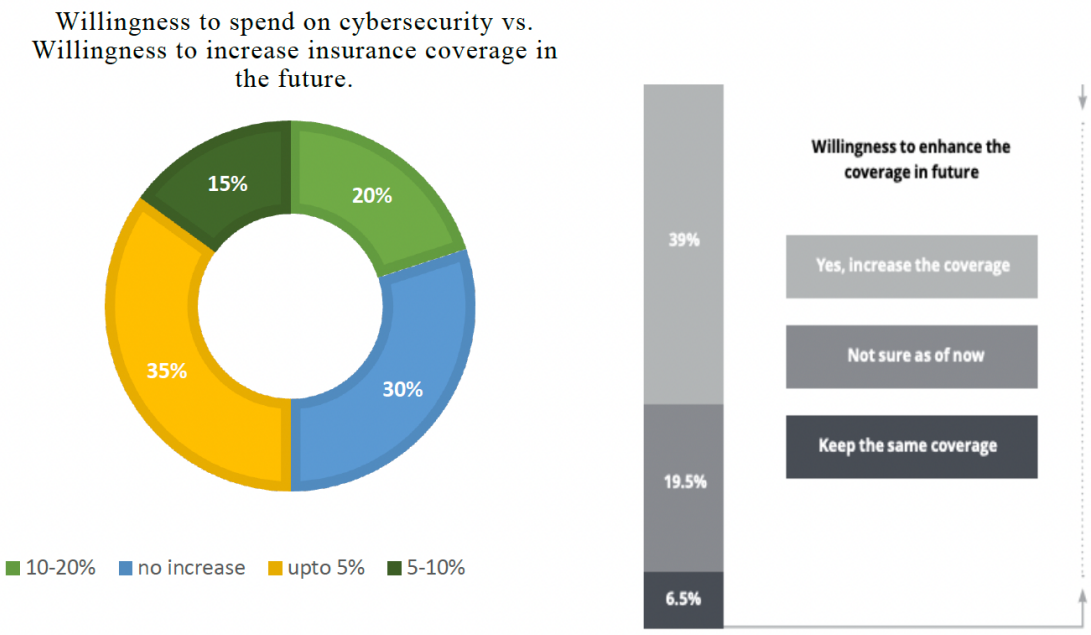
Problems in the development of cyber-insurance :

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?

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 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.



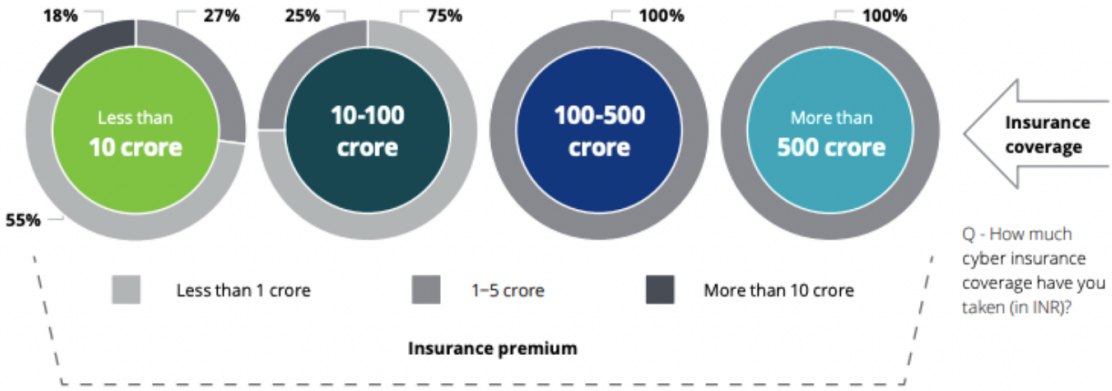
The represented data was presented in the Deloitte Research Survey of 2023, wherein it is evident that a large proportion of the people has lesser interest towards increasing the budget for cyber-security, but on the other hand some have already invested in cyber insurance have the willingness to have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

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 (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.

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

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.

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-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".

1.3 Objectives of the Study

To understand the concept of cyber insurance
To indicate the role of cyber insurance in Indian insurance industry
To know about the current scenario of cyber insurance in India

Chapter 2: Literature Review

2.1 Introduction

We are living in the era of digitalization which has replaced traditional economy of the country. There are many advantages of digitalization like speedy transfer of funds, less time consuming, reduction in transaction costs, transparency, provides new tools which helps to digital marketing etc. But along with the benefits of it there is a possibility of cyber risk. With the demonetization process this risk is increasing day-by- day.

Shree Krishna Bharadwaj H. (2016) has examined cyber liability insurance in India and its growing need. He has focused on various types of cyber risk in business and reasons behind the cyber accountability insurance. He has concluded that cyber insurance has gained its importance in modern society which is run by computers and technology.

Sasha Romanasky, Lillian Ablon, Andreas Kuehn and Therese Jones (2017), have studied on the paper titled "Content analysis of cyber insurance policies: how do carriers write policies and price cyber risk?" The objective of the study is to examine three main components of cyber insurance policies: coverage, applications and rate schedules. They have focused on cyber insurance policies, calculation of cyber risk exposure and premiums and insurer's risk etc. for business in united states of America. They have examined that there is a rising need of cyber insurance in insurance industry and concluded that there is no standardization of policy.

Ceareth W. Peters, Pavel V. Sherchenko, Ruben D. Cohen (2018), have studied on the topic of "understanding cyber risk and cyber insurance". They have discussed in detailed about cyber-crime, cyber risk, cyber insurance and some regulatory perspectives on cyber risk and cyber insurance. They have concluded the current scenario of cyber risk classification and its evaluation as well as challenges faced while collecting data for modeling insurance design. They have also highlighted that the challenges faced by industry and a range of different regulatory guidance documents are not yet standardizes as per the requirements.

Mrs. SreemathiRaghunandanAnd Mrs. KalyaniGorti(2018), have studied o the paper titled "cyber insurance- a growing need". The objectives of the study are to understand digital economy as well as cyber insurance and coverage of and to know about the evaluation and awareness of cyber insurance. They concluded that the concept of cyber insurance is felt only in urban developed areas and few business houses. But there is need to create awareness regarding cyber insurance in rural areas.

G. Nikhita Reddy And G. J. Ugander Reddy,have studied on the paper titled "a study of cyber security challenges and its emerging trends on latest technologies". They have focused on challenges faced by the cyber security on latest technologies as well as techniques, ethics and changing trends of cyber security. They have concluded that there is no perfect solution for cyber-crimes but there should be best try to reduce it in order to safe and secure the future in information technology.

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).

Chapter 3: Research Methodology

This is an applied research. The data has been collected on the basis of various secondary sources like websites, journals, books etc. On the basis of collected data and available information the conclusion has been drawn

Chapter 4: Observations and Analysis

4.1 Observations

When the digital data is accessed by any kind of unauthorized source by using any kind of modern communication network is become cyber-crime. Cyber-crime can be in the form of hacking, virus diffusion, logic bombs, denial of service attack, phishing, web jacking, cyber stalking, data diddling, identity theft, salami slicing attack etc. It is harmful for the individuals, businesses, Government and development of the country. In the first six months of 2017, there were 27,482 cases of cyber-crime and it was reported for every 10 minutes which was 12 minutes in the year 2016. In the past three and half year our country has seen 1.71 lakhs cases of cyber-crime.

According to the article of Bhargav Das Gupta, cyber- crime leads to cyber risk and as it becomes daily event, corporates and insurance companies should work together to fight against cyber-crime because there is a question of cyber- security. Cyber criminals are punished by the cyber laws. But as a solution for victims who are left out, to manage their cyber risk, to reduce the occurrence of cyber-crime and for the purpose of cyber security the role and awareness of cyber insurance in Indian insurance industry becomes useful.

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 organizations1.
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 grew2. 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, there were many spokespersons, but the person who included this topic of cyber-insurance in academic discussions was Bruce Schneider.
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.

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 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.
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.

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 insurance22. 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 cybersecurity 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 today23

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
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 entities24.
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.
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 witnesses25.

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.
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.

4.2 Analysis part :

4.2.1 Concept of cyber insurance

The concept of cyber insurance was emerged in the year 1990s. To understand the concept of cyber insurance in a meaningful way it is necessary to understand the following terms which are related with cyber insurance.

- Digitalization: Digitalization means the process of integration of converting any information in e-format with the help of developed technologies.
- Digital economy:The economy which is based on digital technologies is called digital economy. It is also known as new economy or web economy or Economy based on internet.
- There are three elements of digital economy:

1. E-commerce: E-commerce includes sale and purchase of goods through internet.
2. E-business: E-business includes the whole business is done through computer mediate network.
3. E-business infrastructure: E-infrastructure includes hardware, software and any telecommunication network etc.

- Cyber risk:Cyber risk means the risk of financial loss, damage or disruption to the reputation of business from some sort of failure of its digital system.
- Cyber security:The protection of digital system of any kind of cyber-attacks like interconnected systems of business which includes digital data, hardware as well as software. Cyber security includes various elements like application security, operational security, network and information security etc.

The above terms are interrelated with each other. As a limitation of digitalization cyber-crime takes place and cyber- crime leads to cyber risk which will result into the question of cyber security.

Cyber insurance is a mechanism which secures the victim of cyber-crime by mitigating and providing the coverage against the losses arising out of cyber risk or cyber insecurity or cyber-crime. It provides following coverage against following cyber-crimes i.e. Information Technology Theft Loss Coverage, Malware Coverage, Cyber Stalking Coverage, Identity Theft Coverage, Social Media Coverage, Media Liability Claims Coverage, E-Mail Spoofing Coverage, Cyber Stalking Coverage, Phishing Coverage, Cyber Bullying, Privacy Breach and Data Breach by Third Party.

Cyber insurance can be hack insurance, insurance against first party and third party, insurance against criminal cyber event or fraud and theft of data, insurance against extortion, insurance against computer data loss and restoration, insurance against forensic investigation, insurance against business interruption and reputation insurance.

COMPARATIVE ANALYSIS: BIHAR AND OTHER STATES

Bihar has witnessed a sharp rise in cybercrime incidents in recent years, particularly cases of financial fraud, data breaches, and online scams. According to the Bihar Police Cyber Crime Cell, the state recorded a 60% increase in cybercrime complaints between 2021 and 2023, with most victims being small business owners, students, and rural internet users. A major case in 2022 involved a digital banking fraud in Patna, where thousands of users lost funds due to phishing attacks. The case underscored the urgent need for robust cyber insurance mechanisms to mitigate financial losses.15

While states like Maharashtra and Karnataka have implemented specialized cybercrime response units and have collaborated with insurance firms to promote cyber risk coverage, whereas Bihar lags in such policy interventions. The Bihar government recently launched awareness campaigns on cybersecurity, but concrete policy frameworks encouraging cyber insurance adoption remain absent.16 In contrast, Tamil Nadu has introduced incentives for businesses investing in cybersecurity and insurance, ensuring better financial resilience. This disparity highlights the necessity for Bihar to establish targeted cyber insurance policies and regulatory initiatives to address the growing threat landscape.

COMPARATIVE ANALYSIS: INDIA VS GLOBAL BEST PRACTICES

While India's cyber insurance framework is evolving, jurisdictions like the United States, the European Union, and Singapore have made significant strides in regulating cyber insurance markets. The U.S. insurance sector follows the NIST framework, which provides structured guidelines for cybersecurity risk assessment. Additionally, states such as California have enacted stringent data protection laws, compelling businesses to secure cyber insurance to mitigate financial risks associated with non-compliance.

In the European Union, the General Data Protection Regulation (GDPR) has set a global benchmark for data security and privacy. Companies operating in the EU must maintain cyber insurance policies to address liability arising from data breaches. The GDPR's strict enforcement mechanisms have led to higher claim payouts in cyber insurance disputes, making it a model for India to consider.18

Singapore has also taken proactive steps by mandating cyber risk assessments for businesses seeking cyber insurance. The Monetary Authority of Singapore has worked closely with insurers to develop standardized policy frameworks, ensuring transparency and efficiency in cyber insurance markets.19 Similarly, India could also benefit from adopting similar measures, particularly in ensuring policy standardization and better claims resolution mechanisms.

4.2.2. Role of cyber insurance in Indian insurance industry

In today's world of digitalization, the people are sharing lots of personal as well as financial information through online. More and more people are using smartphones and do various transactions through internet and mobile which can be misused by anyone at any time. India has the largest online market with a wide scope which leads to increases the cases of cyber- attacks and cyber-crimes. So from the view point of financial safety and security, cyber insurance must have included in the financial plan of individuals and businesses. Generally cyber insurance policies are bought by banking and financial services sector but now-a-days it is also taken by manufacturing and pharmaceutical companies. It is not necessary that large scale organizations are the victims of cyber-crime but 60% of

small scale businesses have also felt data breach or data destruction which can damage the reputation of the business. If any individual or business is dependent on IT sector and have heavy online transactions, there is need of cyber protection which is provided by cyber insurance.

The increasing dependence on digital infrastructure has led to a marked rise in cyber threats, affecting industries such as banking, healthcare, e-commerce, and government sectors. Cybercriminals have adopted sophisticated attack vectors, targeting both individual users and large organizations. With the rise of cloud computing, AI (artificial intelligence), and IoT-based operations, the scope of vulnerabilities has widened, making cyber insurance an indispensable safeguard.2

Cyber insurance serves as a crucial mechanism to counter these risks by providing financial indemnity against damages arising from cyberattacks. However, the scope and applicability of cyber insurance policies in India remain limited, with businesses often struggling to interpret policy clauses and eligibility criteria. This lack of clarity is particularly evident in SMEs (Small and Medium Enterprises) and startups, where financial and technical expertise to understand cyber insurance policies remains inadequate.

A significant concern in the Indian cyber insurance market is the lack of standardization in policy wording. Unlike traditional insurance policies, which have well-defined terms and coverage parameters, cyber insurance policies often vary widely in scope. Many Indian insurers follow models inspired by global standards, but gaps remain in terms of policy execution and claims adjudication. The lack of actuarial data on cyber risks further complicates the pricing of cyber insurance policies, leading to inconsistent premiums and coverage benefits across insurers. The Insurance Regulatory and Development Authority of India (IRDAI) has acknowledged these challenges. In its "Guidance Document on Product Structure for Cyber Insurance," the IRDAI emphasizes the need for standardization in policy wording and the development of comprehensive actuarial data to ensure consistent pricing and coverage.3 Additionally, legal disputes arising from ambiguous policy definitions often lead to prolonged litigations and financial losses for the insured.

Despite these challenges, the demand for cyber insurance is growing. Financial institutions, which have been the primary targets of cyberattacks, are increasingly opting for such coverage. With India's digital payment infrastructure expanding, incidents of data theft and financial fraud have surged. Reports indicate that more than 75% of Indian businesses experienced at least one cyberattack in the past year, emphasizing the urgent need for a structured insurance ecosystem to mitigate these threats.4

The insurance sector itself is adapting to these evolving challenges. New products such as ransomware insurance, third-party liability coverage, and crisis response management are being introduced in the market. However, there is a significant gap in penetration, with only a fraction of Indian enterprises opting for cyber insurance compared to global counterparts. This disparity necessitates governmental intervention in promoting awareness and ensuring policy standardization.

LEGAL FRAMEWORK GOVERNING CYBER INSURANCE IN INDIA

The Indian legal landscape for cyber insurance is a composite of statutory provisions, regulatory guidelines, and judicial interpretations. The Information Technology Act, 20005, serves as the primary legislation dealing with cybercrimes and electronic commerce. Sections 43A and 72A6 impose liability on corporations for negligence in handling sensitive personal data. While these provisions establish a basis for liability, they do not explicitly mention cyber insurance as a mitigation tool. The IT Rules, 2011, which define reasonable security practices, have further enhanced regulatory oversight, but their enforcement remains inconsistent.

A significant development is the enactment of the Digital Personal Data Protection (DPDP) Act,

2023. This legislation, which amends parts of the IT Act but does not replace it, introduces a comprehensive data protection regime. It imposes substantial penalties on businesses for data breaches, thereby creating a strong financial incentive for adopting cyber insurance to hedge against the risks of non-compliance. The Insurance Regulatory and Development Authority of India (IRDAI) has issued guidelines to encourage the development of cyber risk policies. However, India still lacks a dedicated, comprehensive framework for regulating cyber insurance contracts, unlike jurisdictions such as the United States, where the National Association of Insurance Commissioners (NAIC) has developed standardized models.

JUDICIAL DECISIONS AND LANDMARK CASES

Several judicial decisions have shaped the environment for cyber insurance in India.

One of the most significant judicial decisions influencing cyber insurance in India is Justice K.S. Puttaswamy (Retd.) v. Union of India (2017),9 which affirmed the Right to Privacy as a fundamental right under Article 21 of the Constitution.10 This landmark ruling created the constitutional foundation for data protection legislation and underscored the legal imperative for organizations to protect personal data, directly increasing the relevance of privacy breach liability covered by cyber insurance.

Similarly, in the case of NASSCOM v. Ajay Sood,11 the court addressed cyber fraud concerns, highlighting the liability of intermediaries.

Regarding financial fraud, while specific High Court or Supreme Court rulings directly on cyber insurance are nascent, numerous disputes are adjudicated by Banking Ombudsmen and Consumer Disputes Redressal Commissions. The legal principles in these forums are often guided by Reserve Bank of India (RBI) circulars on 'Zero Liability' and 'Limited Liability' for customers in cases of unauthorized electronic transactions. These circulars place a heavy burden on banks to prove customer negligence, otherwise making the bank liable for the loss. This has driven financial institutions to adopt robust cyber insurance policies to cover potential losses from large-scale phishing, vishing, and online payment fraud.

Also, in HDFC Bank Ltd. v. Girish Kumar,13 where the court deliberated on the bank’s responsibility in ensuring digital transaction security. The ruling emphasized the necessity for financial institutions to adopt cyber insurance policies to protect customers against online fraud.

On the international front, a key case is Sony Corp. of America v. Zurich American Insurance Co…14 The court's ruling, which determined that a standard general liability policy did not cover a major data breach, set a critical precedent. It emphasized the need for specialized, standalone cyber insurance policies with clear terms, a lesson that is highly relevant for the Indian market where policy wording can be ambiguous.

“The Sony case ruling serves as a cautionary tale for Indian businesses relying on general liability policies, reinforcing the necessity of specialized cyber coverage.”

POLICY RECOMMENDATIONS:

To address the identified gaps and build a robust cyber insurance ecosystem, this paper proposes the following targeted legal and regulatory reforms:

1.Mandate Policy Standardization via IRDAI

A significant concern in the Indian market is the lack of standardization in policy wording, which leads to ambiguity and prolonged litigation. The Insurance Regulatory and Development Authority of India (IRDAI) should move beyond guidance documents and develop mandatory templates for cyber insurance policies. Drawing inspiration from the standardized models developed by the NAIC in the United States and frameworks in Singapore, these templates would ensure clarity, facilitate easier comparison for businesses, and streamline the claims resolution process.

2.Establish a National Cyber Risk Database

The lack of actuarial data on cyber risks leads to inconsistent premiums and complicates the pricing of policies. To solve this, a centralized, anonymized national database of cyber incidents and claims should be established, possibly under the purview of IRDAI or CERT-In. Mandatory reporting of breach data by insurers and corporations would build the necessary actuarial foundation for fair pricing and help in the development of more tailored insurance products.

3.Implement State-Level Incentive Programs for SMEs

There is a significant gap in cyber insurance penetration, particularly among SMEs who lack financial and technical expertise. Following the proactive model set by Tamil Nadu, other states, especially those with rising cybercrime like Bihar, should introduce incentive programs. These could include tax credits or subsidies for SMEs that invest in certified cybersecurity measures and purchase a standard cyber insurance policy. This would directly address the need for governmental intervention to promote awareness and adoption.

4.Formally Recognize Cyber Insurance in the IT Act

While the Digital Personal Data Protection (DPDP) Act, 2023, creates a strong financial incentive for adopting cyber insurance, the primary legislation, the Information Technology Act, 2000, does not explicitly mention it as a mitigation tool. An amendment should be made to the IT Act to formally recognize cyber insurance as a component of "reasonable security practices" under Section 43A. This would provide stronger statutory backing and embed insurance as a key element in corporate cyber governance.

4.2.3. Current scenario of cyber insurance in India

The aim of cyber-crime is financial gain through cyber- attacks on individuals and businesses.

As we already know the recent incidents of cyber-attack left Pune based cosmos bank taking rupees 94 crores hit and from the account of union bank of India 171 million rupees was debited through hacking in the year 2017 which was one of the major incident of cyber-crime. Later this money was retrieved back with the help of government agencies**.**

As per the data provided by Indian Computer Emergency response team (CERT-In), the cases of cyber-attacks are increasing now-a-days. In the year 2014 there were 44,679 cases reported which was

increased to 53,081 in the year 2017.

TABLE: 1

YEAR	CASES OF CYBER ATTACK
2014	44,679
2015	49,455
2016	50,362
2017	53,081

(reddy d. n., 2018)

Along with the cyber-attack the cases of cyber-crime are also increasing. As per the data provided by NCRB (The National Crime Records Bureau), there were 9,622 cases of cyber-crime in the year 2014 which was increased to 12,317 in the year 2017.

TABLE:2

YEAR	CASES OF CYBER CRIME
2014	9,622
2015	11,592
2016	12,317

(reddy d. n., 2018)

India has the second largest online market with a wide scope which leads to increase the cases of cyber-attack and cyber-crime. Netrica consulting India, CyberOps, ALTEN Calsoft Labs, Valency networks and Hicube are the companies which provides services related with cyber security in India.

Bajaj Allianz General Insurance Company Limited, HDFC Ergo General Insurance Company Limited and ICICI Lombard General Insurance Company Limited are the companies of India which offer the service of cyber insurance policies to individuals and corporates at very affordable premium prices starting from as low as Rupees 1000 and going up depending on sum insured and other aspects. After the implementation of personal data protection bills, there is 30% of growth is noticed in the sales of cyber insurance policies.

According to the report provided by the global insurance brokers, there is 25% of cumulative growth in the number of cyber insurance policies reported over the last 4 years.70% of the companies have transferred the threat of cyber-attack to the third party insurance companies.

Mostly cyber insurance policies have been bought by many banks and financial service sector companies. But now it is the requirement of manufacturing as well as pharmaceuticals sector also. In 2017, cyber insurance cover was bought by 250 companies including some of the top banks in India.

As compared to the year 2016, there was rise of 50% in the demand of cyber insurance in the year 2017. The size of cyber insurance premium was Rupees 200 crores in the year previous year which is expected to rise to Rupees 400 crores in the next two years. As compared to other insurance products cyber insurance product has relatively small proportion in the insurance industry. But as the cyber-crime is increasing day- by-day, the cyber insurance has wide scope in future in Indian insurance industry.

4.2.4. CYBER-NSURANCE: EXPLANATION AND THE CURRENT STATE

Cyber-insurance has been available since the 1990s.[1] Despite this long history, cyber-insurance has not yet taken off.

The cyber-insurance penetration rate is especially lower among small and medium sized enterprises (SMEs). In most OECD countries, the penetration level for stand-alone cyber-insurance among large companies was reported to be above 50% in 2017. The proportions of SMEs with cyber-insurance were in the single digits. Among big companies, data intensive companies exhibit a higher propensity to buy cyber-insurance. In India, only banks and ecommerce companies were reported to have cyber-insurance with large coverages.

Cyber-insurance provides coverage for the theft or loss of first-party and third-party data, as well as support services.2 For the loss or theft of first-party data, an insurer may cover expenses related to notifying clients regarding the data breach, purchasing credit monitoring services for affected customers, extortion, and launching a public relations campaign to restore the company's reputation following a cyberattack-led negative publicity.

Third-party cyber-insurance protects a firm from being accused in case of a breach. Third-party coverage includes claims related to unlawful disclosure of a third-party's information and infringement of intellectual property rights. It may also protect if

an insurance holder's weak cybersecurity practices result in passing malware or virus to another user.3

Support services can help limit losses after a cyberattack. They cover expenses such as those related to public relations, IT forensics, and hiring experts in crisis management.

Some Challenges

The cyber-insurance industry and market have some major challenges to overcome. First, there is a lack of standardization across the cyber-insurance products offered by insurers. This means that those buying insurance products are required to have a clear understanding of their cyber risk exposures in order to determine the appropriate type as well as the amount of coverage required based on their specific situation.4 According to a survey conducted by Marsh, 49% of respondents said that they had "insufficient knowledge" about their cyber risk exposures to assess the type and coverage of insurances they need.4 Likewise, another survey found that 38% of U.K. companies had insurance that covered all types of cyber-threats. However, most policies were based on inaccurate risk assessments.

Second, the value chain of the cyber-insurance industry is not well developed. There is the lack of clear understanding and knowledge among intermediaries such as insurance brokers and insurance agents. For instance, according to survey conducted by U.K. legal expenses insurer DAS UK Group, and HSB Engineering Insurance, most insurance brokers in the U.K. were reported to view cyber-insurance as a key and growing market. Nevertheless, one third of them admitted that they had a "poor" or "very poor" understanding of cyber risks and cyber-insurance.

Third, due primarily to newness and the scarcity of data on cyberattacks and related losses insurers face a high uncertainty in pricing cyber risk coverage. They thus tend to be conservative and overcharge for cyber risk coverage.3 Moreover, various cyber-insurance coverages are separately priced.

Fourth, the existence of externality effects may discourage some firms to buy cyber-insurance. If a minimum level of cybersecurity is required from policyholders, it is likely to improve the security of all Internet users. This will create a free riding problem, which reduces incentives for individuals or firms to get cyber-insurance.

DEMAND- AND SUPPLY-SIDE MODELS AND MEASUREMENT ISSUES

Supply-Side Condition

In order to derive a risk-adjusted return on capital, insurance companies need to determine the economic values of the capital invested and earnings. Put simply, the economic value of earnings is equal to cash flow plus the change in the economic value of the assets minus the change in the economic value of liabilities.5 Expressing in a simple equation, it is commercially viable for the insurance company if
Insurance premium > expected loss + risk margin + administrative costs.
(1)
The risk margin in (1) represents an additional amount that investors in an insurance company require so that a return is expected for placing their economic capital at risk.5 The risk associated with a policy is a function of many factors such as the company's industry, data risks and exposures, current practices, and financial health.5 Among the biggest challenges facing the cyber-insurance industry and market is the lack of well-developed mechanisms to actuarially assess and price cyber risks.
Firms face heterogeneous cyber risk environments. In order to understand the essential components and the context of cyber risks, a process-based mode of such risks could be helpful. In such a model, risk equals "threat plus vulnerability plus consequences. A threat is a danger related to cyber-attack that has the potential to cause harms to an organization. For instance, factors such as a firm's jurisdiction, physical location, nature of business, political orientation, and symbolic significance affect the degree of cyber-threats.
Cyber-vulnerability refers to the degree to which an organization is susceptible to harm from cyber-attacks. For instance, a firm with a poor cybersecurity practice is more likely to be harmed by cyber-criminals.

Finally, consequences of possible cyberattacks need to be evaluated in terms of factors such as reputational damage, financial loss, and possible physical harm. More severe consequences can arise if the jurisdiction of the firm's operations has strict laws against companies' failure to protect personally identifiable information.
Proper assessment of cyber-threat, cyber-vulnerability, and consequences of cyber-attacks are needed to gain a better understanding of cyber risks facing the firm. Insurance companies have realized that there is a fundamental need for better risk assessment tools.
On the plus side, there have been efforts to develop better analytical approaches, improving data collection efforts, and sharing relevant data with other players. When insurers model and test more information, insurance products are likely to be sold at more reasonable prices. Insurance companies are also taking measures to address legal uncertainties.1
Demand-Side Condition
A customer will invest in cyber-insurance if expected utility without cyber-insurance < expected utility with cyber-insurance (2)
Alternatively, the demand-side condition can also be written as
U(Benefits of insurance) > U(Costs of buying an insurance plan).(3)
U(*) is a utility function, which evaluates a cyber-insurance plan's benefits and costs in a common metric. Firms and individuals invest in cyber-insurance only if its value proposition is clear. A current challenge is that the coverage terms are often complex, which makes it difficult to articulate the value proposition. There is still the lack of data on the odds of companies being victimized, which makes it difficult to estimate the costs of cyberattacks. It is also difficult for companies to measure the nature and extent of cyber-related exposure and to make decisions as to what coverages for how much to purchase. A related point is that some cyber-insurance policy holders find that their insurance does not cover all the losses in case of a cyberattack. To take an example, in December 2013, Target faced a high-profile security breach, which compromised 40 million credit and debit-card accounts and 70 million customers' personal data.

Transaction Costs in Cyber-Insurance Markets

In the context of business transactions involving two or more parties Nobel Laureate Douglas North argues that ".. transaction costs are . . . two things: (1) the costs of measuring the dimensions of whatever it is that is being produced or exchanged and (2) the costs of enforcement." He goes on to say that "a lot of what we need to do is to try to measure the dimensions of what we are talking about in such a way that we can define them precisely."3 Emphasizing the importance of measurements in enforcement, North argues: "Without being able to measure accurately whatever it is you are trying to enforce, there cannot be effective enforcement, even as a possibility."8

A transaction cost problem has two main components: (a) There is the presence of uncertainty and (b) the ability of the policy holder to change her/his behavior without detection.9 Regarding (a), it is worth noting that due to the newness and limited availability of data, there is a challenge in estimating the probability of cyberattacks.

As to (b), a key challenge that insurers face in other types of insurance products is that the behavior of policy holders is often unobservable. Unlike many other insurance products, by working closely with the policy holder, cyber insurers can avoid some of the above-mentioned problems. They can support overall risk management for their clients and tailor cyber-insurance to only residual risks in a cost-effective manner. For instance, using specialized software, insurers can remotely check whether policyholders have up-to-date software and defense mechanisms in place.1 There has already been some progress on this front. Companies with strong cybersecurity practices pay lower insurance premiums.1

The above-mentioned feature also leads to a lower enforcement costs. A second-party enforcement, in which one party retaliates against the other (e.g., a cyber insurer penalizing a cyber-insurance policy holder for having a poor defense measure), can especially be more easily carried out in the context of cyber-insurance. It reduces the risks of policyholders failing to protect themselves against cyberattacks, thinking that they are covered against losses associated with such attacks.

4.2.5. A Utility Model for Cyber-risk

The Critical Success Factor (CSF) of most organisations today is proper functioning of computers, online data retrieval and robust scalable communication channel (like the Internet). The success of e-commerce, in particular, lies in its easy visibility for 24 X7 over the Internet. The Internet today is widely used the world over by both households and industry. Many a traditional brick and mortar company like Nestle (Glick, 2001) and Philips have implemented ERP packages which integrate their backend production units and front-end sales force. But the success of such an automated supply chain management lies solely on the internet/network channels. Similarly, most financial service providers like banks and insurance, provide customers a basket of online services. These services not only benefit customers but also reduce the costs for companies. There has also been a marked growth of virtual (online) companies, like e-Bay, Amazon.com etc. A study by Forester (Burner, 2003) reveals that online retail sales in USA in 2003 were $95.7 billion while it is projected to be $229.9 billion by 2008.

A company like Amazon.com, which exists solely in cyberspace, would face a total loss of revenue should a hacker manage to shut down its operations. To add to this are virus attacks. Table 1 illustrates some notable instances of losses suffered by financial organizations the world over due to hackers and virus attacks.

the use of insurance as a supplementary tool to reduce the financial losses suffered due to e-risk. This would help reduce the financial burden on the organisations, as the insurance company would indemnify the loss. In effect, an organisation's risk is being passed on to another party on paying a premium. This reduces the companies concern about "self insuring" i.e, keeping aside huge amounts for contingency purpose. This, in turn, is good corporate strategy, as huge amounts are not locked away for contingency recoveries. Using utility theory, we find out the premiums an insurance company charges, based on the risk profiles (risk averse ,risk neutral and risk seeker) of its clients in case of business revenue loss due to the

failure of an Internet Service Provider (ISP). We also provide the traits of the e-risk insurance product that an insurance company can use.
The next section defines e-risk and the present e-risk products available globally. This is followed by a brief review of the related work in the area of e-risk quantification. Next, the premium that an organisation, would be ready to pay (based on their risk profile), to reduce losses due to an ISP failure is modelled and the traits of our proposed e-risk insurance product provided. The concluding remarks are provided in the last section.

Classification of e-Risk Type and Impact

E-risk is defined as the possibility of an event, whose occurrence causes loss to business. Some very common types of e-risk items that an organisation is exposed to are as follows:
(i) Compromise of network security components like firewall, proxy servers, anti virus and infecting the server with virus or unauthorized access;
(ii) The web server of an organisation is compromised, and incorrect or indecent material displayed on the web site;
(iii) Service providers (i.e. Application Service Provider (ASP) or Internet Service Provider (ISP)) fail;
(iv) Identity theft, i.e., confidential customer information is hacked from an organisational database (for example, pin numbers of credit cards from a bank);
(v) internal attacks by disgruntled employees;
(vi) Cyber-Extortion;
(vii) Denial of Service (DOS), by making malicious calls to the router.
The impact of e-risk can also be broadly classified as, firstly, loss due to direct compromise of the information asset (data/bandwidth). This leads to confidentiality, integrity and availability violation of the information asset. Secondly, indirect loss to an organisation through service interruption, i.e., denial of service (DOS), loss of competitive advantage, slander of website, legal liabilities (Johnson, 2002; Rowen.)

e-Risk Insurance products: The present market scenario

Insurance companies like AIG and Lloyds have introduced a number of products to guard against e-risk. These e-risk products are, till date, confined to the UK, USA and Japan. AIG's e-assurance product is called e-advantage (www.aignetadvantage.com) The product comes in seven flavors i.e., Ordinary, Professional, Commercial, Liability, Property, Security and Complete.
AIG provides coverage against 13 types of e-risk. Fig 2.illustrates the relative importance attached to each of these risks by AIG. It is evident from Fig 2 that Cyber-Terrorism coverage is available from all of AIG's products. This is followed by web content liability and damages due to legal suits.
A recent survey (www.insurancejournal.com) has revealed that Business Interruption insurance policies are held by fewer than 24% of businesses. Only 18% have Crime Loss insurance. Less than 13% of employers have Unauthorised Access insurance. Fewer that 6% have Crisis Communications insurance to cover property loss following e-disasters. And not even 2% have Extortion and Reward insurance to cover costs associated with cyber-terrorism. This clearly indicates that e-risk insurance is not popular with the corporate world.

e-Risk quantification: Related Work

Radcliff (2001) states that e-risk models so far have been qualitative as there is a dearth of historical data on claim frequency and claim amount. He suggests the need to develop actuarial tables by quantifying the risks. Grzebiela (2002) identifies e-risk in terms of technical risk, personal information loss risk, economic risk and societal risk. Gordon et-al (2003) provides a framework that an organisation should follow for choosing a cyber-risk protection policy. Matthias et. al. (2002) have classified e-risk in terms of strategic risks, operational and systems risks, legal and regulatory risks and financial risk but have not come up with any quantification of e-risk. Little work has been done with regard to quantifying the risks in terms of the expected loss. Similarly, no work has been done to model the probability distributions of the claim frequency and the claim severity.

e-Risk Modelling: The Utility Approach

We assume a user (household /organisational) having an initial wealth of W, is connected to the Internet through an ISP. The user is exposed to risks of hacking, virus attacks or failures (own machine, ISP or network). These are bound to cause financial losses. To protect against these, the user might choose to insure or bear the entire risk alone. Table 3 illustrates the scenarios that a user (who has insured) can meet, the details about the probabilities of the occurrence of these events, the expected losses and the premium paid.

Table 3: The outcome probabilities of an insured user

Slno	Scenarios	Probabilities	Loss	Premium	Total Utility
i)	ISP down and user down	$P(I_D, U_D) = a$	X	M	W-M-X+X
ii)	ISP up but user down	$P(I_U, U_D) = b$	X_U	M	$W-M-X_U+X_U$
iii)	ISP down but User Up	$P(I_D, U_U) = c$	X_I	M	$W-M-X_I+X_I$
iv)	ISP up and User Up	$P(I_D, U_U) = d$	0	M	W-M

In all the cases (Table 3) the utility of the user goes down only by the amount of premium paid (M), as the insurance company indemnifies the loss (X). Table 4 illustrates the scenarios that a user (who is self insured) can meet and provides the details about the probabilities of the occurrence of these events, the expected losses and the premium paid.

The utility of the uninsured user (Table 4) goes down by the amount of loss incurred i.e., either through the user's machine failure or ISP being down or both being down. While if both the user and ISP machines are up, then there is no loss to the users in initial wealth.

Table 4: The outcome probabilities of a "self" insured user

Slno	Scenarios	Probabilities	Loss	Premium	Total Utility
i)	ISP down and user down	$P(I_D, U_D) = a$	X	0	W-X (where $X = X_U + X_I$)
ii)	ISP up but user down	$P(I_U, U_D) = b$	X_U	0	$W-X_U$
iii)	ISP down but User Up	$P(I_D, U_U) = c$	X_I	0	$W-X_I$
iv)	ISP up and User Up	$P(I_D, U_U) = d$	0	0	W

A rational decision maker would only insure if the utility arising from insurance were greater or equal to the utility obtained from non-insuring. Using this basic premise of utility theory, we arrive at the expected premium for a user.

Table 6: Risk premium vis-à-vis risk profile

Risk profile	Utility function	Total Loss	Expected Loss	Maximum Premium
Neutral	$U(W) = W$	5000	50	50
Constant Risk Averse	$U(W) = 1 - e^{(-W/1000)}$	5000	50	908

It is evident that the risk neutral person would not invest in the insurance policy. While the risk averse user would be ready to pay as high as Rs 908 to be covered by insurance.

e-Risk Insurance product characteristics

An insurance company would cover E-risk because, firstly, the probability of the event(s) (i.e. breakdown of network or jamming of a network or a virus attack) leading to loss incurrence is relatively small. Secondly, there is available a large number of similar risks for pooling and for reduction in the variance of experience. This is possible as a large number of organisations the world over are dependent on online transactions. Thirdly, as the loss involved due to breakdown of a network or jamming of a network is financially large, organisations have substantial "insurable interest" to reduce it. Fourthly, the risks/losses of network failure or DDOS (Distributed Denial of Service) are independent from that of any other type of general insurance product (like Property, Liability, Financial loss, Fixed Benefit). Fifthly, the insurer can accept such a risk as it is quantifiable and an upper limit of possible liability can be fixed. Sixthly, the insurer can assume that moral hazard would mostly be absent.

The existing general insurance products like Property, Liability, Financial Loss and Fixed Benefit (Rowen, 2000) cannot provide much relief to an insured, against the peril of network jamming and, thereby, lead to a substantial loss of revenue. A new product is warranted to guard the online users. We suggest the characteristics of a new general insurance product to protect commercial users from the perils of cyberrisk. High moral hazard arising from information asymmetry prevents us from covering the household users by this new proposed policy. The usage and the loss patterns of a household user are difficult to estimate. A brief discussion of the traits of the proposed policy follows.

A. Benefits and Perils:

Perils related to cyber risk are, firstly, business interruption due to failure of software or hardware or virus attack or DDOS. Secondly, loss to a third party due to virusinfected mail sent to them or due to downloading of a document or clicking on a hyperlink on a website. The product should have the provision of indemnifying the first and third party, which has suffered consequential losses due to business interruption. We propose levels of benefits as either third party or comprehensive (i.e. compensation for both first and third party losses). The product would additionally have a provision for indemnifying the first party for any loss suffered to its hardware components.

B. Measure of Exposure:

It is a measure that insurance companies use for determining the amount of risk associated with each policy. It is needed for setting a premium on products. Generally such measures need to be, firstly, a good representative of the frequency of claim and the severity of claim. In short, the total expected claim amount could be proportional to the exposure. Secondly, the measure should be easily obtainable and verifiable. In the case of e-risk insurance, the best measure of exposure is turnover. Higher turnover for an organisation pursuing e-commerce indicates longer periods of online transactions. Similarly, high turnover brick and mortar organisations using ERP to enhance the supply chain management are also logged to the network for long periods. ISPs having high turnovers too use Internet to provide support to their customers. This in turn increases their chances of damage to the organization's website/ database by hackers, failures, viruses etc.

C. Claim Characteristics:

The claims from an insured online user machine, being hacked or facing a DDOS, would usually be reported immediately. While the claims for damage to third parties (e.g. a virus in a mail attachment) would take a slightly longer time to settle. Mostly, the claims are short tailed. Businesses doing online transactions would be more prone to cyber risk than ordinary users, as the length of use of computers is higher in an organisation.

D. Risk and Rating Factors:

Exposure measures are not good measures of risk. Refinement in premium calculation is done by using parameters like risk factors and rating factors. Risk factors if present can lead to peril. Risk factors affect both claim frequency and claim severity. But in some cases, these risk factors are not objectively measurable. Then, proxy parameters called rating factors are used for premium calculation. Otherwise, risk factors and rating factors are the same.

The risk factors in case of e-risk are as follows:

a) the number of hours of online transaction
b) the ease with which the website can be hacked and cost of repairing it
c) the vulnerability of the ISP's /users' equipment (like routers gateways)

d) virus attack risk
e) software or hardware failure risk
f) the throughput of the server of the user/ISP
g) the websites accessed by the user

Some rating factors related to e-risk insurance are as follows:
a) type of cover (first party or comprehensive)
b) excess (i.e. the proportion of risk passed for pooling)
c) the value of the contents of the website and its importance to the organisations revenue earnings.
d) age of the user
e) the purpose of use (i.e. " business" or "domestic")
The rating factor 'the purpose of use (i.e. "business" or "domestic")' acts as a proxy for the risk factors like "number of hours of online transactions" and "virus attack risk". Similarly, the rating factor "age of the user," is an effective proxy for the "the websites accessed by the user" "number of hours of online transactions" and "virus attack risk". The "type of cover" is an important rating factor since users with comprehensive cover would have greater propensity to be careless than those insured with first party cover. This is so the insurance company would indemnify all losses to both self and third party holding comprehensive cover vis-à-vis only first party losses in the case of first party cover. The rating factor "the value of the contents of the website and its importance to the organisations revenue earnings" is important since organisations doing online transactions attach a very high importance to their websites and online databases.

Exclusion:

For any situation where the insured is in possession of more information about the likelihood of the claim, the insurer would not provide for any compensation. These include self-inflicted loss, accessing insecure websites, act of terrorism etc.

Chapter 5: Findings

- Cyber-crime is big emerging issue for the management of cyber risk.
- The proportion of cyber-attacks and cyber-crimes are bound to increase as compare to present scenario in near future which will result into increase in the more demand of cyber insurance policies.
- The growth of digitalization emerged the need of cyber insurance in India which is beneficial to individuals, businesses, government as well as educational institutions also.
- The awareness regarding risk of cyber-crime and cyber insurance is very low in India which is a challenge for insurance companies.
- There is a scope to cover rural areas with more strengthen and secured banking system through cyber insurance.
- Only three companies are providing cyber insurance in India thus other insurance companies should be motivated

Chapter 6: Conclusion and Summary

6.1 Conclusion

Cyber-insurance market currently accounts for a vanishingly small proportion of the total insurance market. Nonetheless, it is growing fast. There are challenges associated with actuarially estimating the likelihood of cyberattacks and the total anticipated costs of such attacks. The lack of relevant data has led to an inaccurate assessment of cyber risks and higher premiums. On the plus side, insurers can remotely monitor policyholders' cyber-defense mechanisms. It provides a low-cost mechanism for a second-party enforcement. It is important to have a thorough understanding of the multifaceted nature of loss in case of cyberattacks. For non-IT businesses, first-party cybersecurity insurance could be enough, but third-party cybersecurity insurance may be needed for firms dealing with sensitive data of customers. Since most current policies are bespoke in nature, firms need to look for policies that are based on the need rather than the cost. Due to the lack of prior experience, potential clients do not immediately understand the value proposition of cyber insurance. It has resulted in low demand. Cyber-insurance education and awareness can make a big difference. A higher public awareness of cyber security risk and a higher degree of understanding of the sophistication of cyberattacks can also stimulate the demand of cyber insurance. Firms should be convinced that the value proposition of insurance is interesting for them. Insurers need to make sure that potential clients get a simple and clear explanation of benefits from their cyber insurance. It is important to take measures to increase perceived economic benefits of cyber insurance. Insurers must consider new market segments that are not currently investing in cyber insurance. They need to pursue firms in industries low digitization, households, and SMEs. Data protection regulations that require financial protection against cyber-related losses could also lead to the growth of the cyber-insurance market. Finally, proper regulations may address the free-riding problem. Measures such as those already taken indicate that there have been some initiatives on this front.

Summary

As a growing challenge of cyber risk, cyber insurance is very useful insurance product and plays a vital role in Global insurance industry. It is important to take measures to increase perceived economic benefits of cyber insurance. Insurers must consider new market segments that are not currently investing in cyber insurance.

References

1. Journal Article with DOI

Cyber risk. (n.d.). Retrieved october 19, 2018, from www.therim.org: https://www.therim.org/Knowledge-and- resources/thought-leadership/cyber-risk/

Digital economy . (n.d.). Retrieved october 19, 2018, from www.google.co.in: https://www.google.co.in/search?q=digital+economy+meanin g&oq=digital+economy+meaning&aqs=chrome..69i57j013.8969j0j7&client=ms-unknown&sourceid=chrome- mobile&ie=UTF-8

2. Conference Paper

Economictimes. (n.d.). Retrieved october 25, 2018, from m.economictimes.com: https://www.google.co.in/amp/s/m.economictimes.com/indus try/banking/finance/insure/demamnd-for-cybre-cover-jumps-50/amp_articleshow/62360112.cms

Reddy, d. n. (2018, september 10). newindianexpress. Retrieved october 24, 2018, from www.newindianexpress.com: https://www.google.co.in/amp/www.newindianexpress.com/b usiness/2018/sep/10/Cyber-insurance-to-soon-become- must-have-for-all-individuals-1869839

More References:

1. iif.com, “Cyber risk insurance: A growth market adapting to a changing risk,” Insti. Int. Finance, Washington, D.C., USA, Dec. 7, 2017.
2. 2. C. P. Baban, Y. Gruchmann, C. Paun, A. C. Peters, and T. H. Stuchtey, “Cyber insurance as a contribution to IT risk management: An analysis of the market for cyber insurance in germany,” 2017, Brandenburg Inst. Soc. Security gGmbH
3. L. DeFranco, “What you need to know about cybersecurity insurance,” 2017. Available at https://blog.abacus.com/basics-of-cybersecurity-insurance/
4. Marsh & McLennan Co., “Cyber risk in Asia-Pacific the case for greater transparency risk in focus series,” 2017.
5. L. Rubin, M. Lockerman, R. Tills, and X. Shi, “Economic measurement of insurance liabilities: The risk and capital perspective,” 2009. Actuarial Practices Forum.
6. H. P. Binswanger-Mkhize, “Is there too much hype about index-based agricultural insurance?” J. Dev. Studies, vol. 48, no. 2, pp. 187–200, 2012.
7. D. S. Nagin and G. Pogarsky, “Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence.” 2001. Available at http://onlinelibrary.wiley.com/doi/10.1111/j.1745-9125.2001.tb00943.x/abstract
8. D. C. North, “Dealing with a nonergodic world: Institutional economics,” Property Rights, Global Environment: Duke Environment, Law, Policy Forum, vol. 10, no. 1, pp. 1–12, 1999.
9. D. W. Allen, “Transaction costs,” in B. Bouckaert and D. G. Gerrit, Eds., The Encyclopedia of Law and Economics. Chelthenham, UK: Edward Elgar, 2000, vol. 1, pp. 893–926.
10. Ruperto P. Majuca, W. Y. (n.d.). The Evolution of Cyberinsurance.
11. Camillo, M. (2017). Cyber risk and the changing role of insurance. Journal of Cyber Policy,

12. 53-63.
13. Mosleh, N. (2019, February). Impact of Technology on Insurance Industry. Impact of
14. Technology on Insurance Industry, pp. 2-28.
15. Martin Eling, M. L. (2017). The Impact of Digitalization on the Insurance Value Chain and the
16. Insurability of Risks . The Geneva Papers on Risk and Insurance.
17. Ranjan Pal, L. G. (2014). Will Cyber-Insurance Improve Network Security? IEEE Conference
18. on Computer Communications (pp. 235- 243). IEEE Conference on Computer
19. Communications.
20. Miller, L. (2019). Cyber Insurance An Incentive Alignment Solution to Corporate Cyber-
21. Insecurity. Journal of Law & Cyber Warfare, 147-182.
22. Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional
23. analysis. Elsevier Ltd.
24. Deloitte. (2023). Cyber insurance in India: Navigating risks and opportunities in a digital
25. economy. Deloitte Survey Report .
26. Lall, S. (2023, December 10). The Economic Times. Retrieved from
27. Economictimes.timesindia: https://bfsi.economictimes.indiatimes.com/blog/cyberinsurance-
28. an-evolving-story/105867676
29. Singhel, T. (2023, August 20). The Economic Times. Retrieved from
30. economictimes.indiatimes:
31. https://economictimes.indiatimes.com/markets/stocks/news/how-ai-blockchaintechnology-are-taking-indias-insurance-industry-to-nextlevel/articleshow/102872373.cms?from=mdr
32. Chin, K. (2024, january 18). upguard. Retrieved from upguard.com:
33. https://www.upguard.com/blog/cybersecurity-regulationsindia#:~:
34. text=The%20IT%20Act%20of%202000,protection%20policies%2C%20and
35. %20govern%20cybercrime.
36. India, G. o. (2024, March 20). Ministry of Electronics & Information Technology. Retrieved
37. from meity.gov: https://www.meity.gov.in/content/cyber-laws
38. Christian Biener, M. E. (2014). Insurability of Cyber Risk: An Empirical Analysis. The Geneva
39. Papers on Risk and Insurance - Issues and Practice, 40(1), 131-158.
40. Jayendra Kumar, S. M. (2016). Cyber Risk Insurance-An Indian Perspective. International
41. Journal of Advanced Research, 4(7), 1270-1278.
42. Sood, G. (2014). Comparative Analysis of Cyber Privacy Law in India and in the United States
43. of America. law and politics, 12(2), 129-135.
44. KPMG. (2015). Cybercrime survey report 2015. KPMG.com/in.
45. Cyber Insurance in India: Navigating Legal Frameworks, 4 Indian J. Legal Rev. 80 (2024), https://ijlr.iledu.in/wp-content/uploads/2024/11/V4I480.pdf.
46. The Dark Side of AI: How Cybercriminals Are Exploiting Artificial Intelligence for Sophisticated Attacks, CXO Today (Mar. 3, 2025), https://cxotoday.com/specials/the-dark-side-of-ai-how-cybercriminals-are-exploiting-artificial-intelligence-for-sophisticated-attacks/. This article discusses how AI is revolutionizing cybersecurity—not just for defenders but also for cybercriminals, who are using AI to create highly convincing phishing emails, develop adaptive malware, and launch sophisticated social engineering attacks using deepfake videos and voice cloning.

47. 3 INS. REGULATORY & DEV. AUTH. OF INDIA, Guidance Document on Product Structure for Cyber Insurance (2021), https://irdai.gov.in/documents/37343/365525/Product%2BStructure%2Bfor%2BCyber%2BInsurance2021-09-08.pdf.
48. Over 80% Indian Companies Hit with Cyber Attacks Last Year: Report, Times of India (Sept. 5, 2023), https://timesofindia.indiatimes.com/gadgets-news/over-80-indian-companies-hit-with-cyber-attacks-last-year-report/articleshow/103394017.cms.
49. 5 Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
50. 6 Information Technology Act, 2000, § 43A, § 72A, No. 21, Acts of Parliament, 2000 (India).
51. 7 From Bill to Law: India's Digital Personal Data Protection Journey & Implications, Fortune India (Feb. 10, 2025), https://www.fortuneindia.com/opinion/from-bill-to-law-indias-digital-personal-data-protection-journey-implications/120360.
52. Insurance Regulatory and Development Authority of India, Guidelines on Information and Cyber Security for Insurers, IRDAI (2023), https://irdai.gov.in/documents/37343/366029/IRDAI%2BCS%2BGuidelines%2B2023.pdf,
53. National Association of Insurance Commissioners, Insurance Data Security Model Law (#668), NAIC (2017), https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf.
54. 9 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
55. 10 INDIA CONST. art. 21.
56. 11 NASSCOM v. Ajay Sood, (2005) 127 DLT 738 (India).
57. 12 Reserve Bank of India, DBR.No.Leg.BC.78/09.07.005/2017-18, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (July 6, 2017).
58. HDFC Bank Ltd. v. Girish Kumar, (2020) 3 SCC 501 (India).
59. 14 Sony Corp. of Am. v. Zurich Am. Ins. Co., No. 650301/06, 2006 WL 145084 (N.Y. Sup. Ct. 2006) (U.S.).
60. 15 Kshitiz, Cyberfraud in Patna: Over 50 Cases Reported in September, Times of India (Sept. 10, 2024), https://timesofindia.indiatimes.com/city/patna/cyberfraud-in-patna-over-50-cases-reported-in-september/articleshow/113830530.cms.
61. 16 Cybercrime Awareness in Bihar: Government Initiatives and Public Response, Suraksha Bharata Awaz (Jan. 27, 2025), https://suraksha.bharataawaz.com/2025/01/27/cybercrime-awareness-in-bihar.
62. 17 GOV'T OF TAMIL NADU, Guidelines for Administration of Incentives & Concessions Announced in the MSME Policy 2021 (2021).
63. What Is GDPR's Impact on Cyber Insurance?, GRC World Forums (Jan. 15, 2024),
64. 19 Singapore: MAS Revises Technology Risk Management Guidelines, Global Compliance News (Feb. 16, 2021), https://www.globalcompliancenews.com/2021/02/16/singapore-mas-revises-technology-risk-management-guidelines280121.