AN ARTICLE ON CYBER SECURITY INSURANCE AND ITS IMPORTANCE IN SUSTAINABLE BUSINESS

Anurag Gourav, Research Scholar, Narayan School of Law, GNSU, Jamuhar, Bihar

ABSTRACT

The infrastructure and services provided by IT have become more and more important to society. Furthermore, the COVID-19 pandemic compelled a change from the conventional method of working, which required physical presence, to a more contemporary and adaptable method, which involves working remotely. As a direct result of the larger attack surface, this has increased the frequency of cyberattacks, but it has also increased the need for information system protection. When it comes to information system protection, cyber insurance is taken into consideration as a risk management tactic. Cyber insurance is becoming a vital tool for defending businesses against financial losses brought on by cyberattacks. Identity theft, Cyberstalking, Malware attacks, Phishing, Cyber extortion, Privacy and data breach by third parties are some of the crimes which are mainly effected by cyber-criminal. India has a strong legislative toolkit to prevent cybercrimes and protect cybersecurity. The foundation for the nation's cyber security laws is laid by two significant cyber laws: the Information Technology Act of 2000 and the IT (Amendment) Act of 2008. The Digital Personal Data Protection Act (DPDP) 2023, which attempts to control the way entities handle users' personal data, may incentivize businesses to get cyber insurance in order to reduce the risk of financial loss from liabilities. India's ever-changing digital environment necessitates a proactive approach to cybersecurity. Businesses must be aware of cybersecurity laws and obtain cybersecurity insurance in order to defend themselves against constantly changing cyberthreats. Organizations can confidently navigate the cyber legal landscape and create a secure digital future by adhering to regulations and maintaining sufficient insurance. To draft the current landscape, I have reviewed the relevant articles on cybersecurity insurance, relevant laws and practice in this sector.

Keywords: Cyber Security, Phishing, Cyber Laws, Insurance

Introduction

Cybercrime is becoming more common and more severe as a result of globalization, digitization, and smart technologies. Strong cybersecurity defence systems are important, even if this is a new area of study and business. This has been noted at the corporate, national, and international levels. Businesses are shielded from financial damages by cybersecurity insurance against a variety of situations, including, system hacking, data breaches, ransomware payments, and theft.[1] You should have at least some cyber insurance coverage if you run a small business and hold sensitive data on a computer or online.

In the early 2000s, insurers started paying for a portion of the damages brought on by a data breach in conventional business insurance plans.[2] These early, very basic plans usually covered losses from digital or electronic assets, extortion, and business interruption. Driven primarily by stringent reporting requirements and heightened regulations, enterprises have expanded their approaches to cyber mitigation to better match their risk management practices.[3] It makes sense for enterprises to integrate insurance as one of their mitigation options when they manage cyber risk in the same manner that they handle other threats. An company can assist cover its financial losses in the case of a cyberattack or data leak by purchasing cyber insurance. Additionally, it assists companies in defraying any expenses associated with the remediation process, including paying for the investigation, crisis management, legal counsel, and customer refunds.[4]

Meaning and importance of Cybersecurity Insurance

Operational risks to information and technology assets that have an impact on the privacy, accessibility, and/or integrity of data or information on systems are referred to as cyber risks.[5] Cyber insurance is an insurance policy intended to shield policyholders from cybercrimes, according to the Insurance Regulatory and Development Authority of India (IRDAI), which is in charge of overseeing and controlling the country's insurance and reinsurance markets.[6] Cyber

---

[1] Whitney Vandiver, Cybersecurity Insurance: What It Covers, Who Needs It, NERDWALLET (Aug. 21, 2024, 10:04 AM), https://www.nerdwallet.com/article/small-business/cybersecurity-insurance

[2] Steven Bowcut, What is cybersecurity insurance and why do people need it, CYBERSECURITYGUIDE.ORG (Aug. 21, 2024, 10:04 AM), https://cybersecurityguide.org/resources/insurance/

[3] ibid

[4] What Is Cyber Insurance? Why Is It Important?, FORTINET(Aug. 21,2024, 10:04 AM) https://www.fortinet.com/resources/cyberglossary/cyber-insurance

[5] Mr Rohit Kumar Sharma, Bridging Gaps in Cybersecurity with Cyber Insurance, INSTITUTE FOR DEFENCE STUDIES AND ANALYSES, (Aug. 21,2024, 10:04 AM) https://idsa.in/issuebrief/Bridging-Gaps-in-Cybersecurity-with-Cyber-Insurance-RSharma-210324

[6] ibid

insurance offers defence against future third-party claims and liabilities arising from such occurrences in addition to addressing or mitigating the financial damages directly caused by a cyber destruction. Consequently, it is possible to classify coverage for losses resulting from cyber incidents by distinguishing between losses that are directly attributable to the occurrence (first-party coverage) and losses that are the consequence of lawsuits brought by harmed parties (third-party coverage).[7]

The need for cyber insurance is growing for all businesses, as the possibility of cyberattacks targeting users, devices, networks, and applications increases. This is due to the fact that data compromise, loss, or theft can have a serious negative effect on a company, resulting in everything from clientele loss to revenue and reputation loss. Businesses might also be held accountable for any harm brought about by the loss or theft of data belonging to third parties. A cyber insurance policy can assist in the remediation of security incidents and safeguard the company against cyber events, such as acts of cyberterrorism. For instance, 77 million users' data was exposed in 2011 when hackers gained access to Sony's PlayStation Network.[8] Users of the PlayStation Network were also unable to access the service for 23 days due to the attack. Cyber insurance could have prevented Sony from having to pay over $171 million in expenses[9]. But since it lacked a policy, it was forced to pay for the entire cost of the cyber damage.

Businesses which needed Cybersecurity Insurance

Practically every type of business, regardless of size, is susceptible to cybercrime. However, cybersecurity insurance is particularly crucial for:

- Companies that keep sensitive data on computers or the internet. You run the risk of a cyberattack if your company keeps sensitive information on file, like credit card numbers, phone numbers, or Social Security numbers. These company should consider cyber insurance policy. If a institution store sensitive data of customers.

- Companies with sizable clientele. Following a data breach, insurance can help cover some of the regulatory fines that these businesses may be subject to. State laws frequently mandate that businesses notify customers of data breaches; first-party

[7] ibid
[8] What Is Cyber Insurance? Why Is It Important?, FORTINET(Aug. 21,2024, 10:04 AM) https://www.fortinet.com/resources/cyberglossary/cyber-insurance
[9] ibid

policies can pay for this expense, which can add up for businesses with sizable customer bases.

- Companies that make a lot of money or have valuable digital assets. The expenses linked to cyber incidents can be unpredictable, and larger businesses are probably in possession of more valuable data, which may be subject to a higher ransom.

Features and advantages of Cybersecurity Insurance

Policies for cyber insurance now provide coverage that goes beyond data breaches. They provide defence against a variety of online dangers. The following are a few threats for which coverage might be offered.

- Ransomware: Payments for ransomware and other forms of cyber-extortion are frequently covered by insurance. Malware is a common tool used by criminal elements to prevent users from accessing their systems and to threaten to reveal private information to the public.[10] Police authorities advise against paying ransoms to victims due to the lack of assurance that the hackers will remove malicious software or recover data.
- Social engineering attacks and business email compromise (BEC): A lot of cybersecurity policies address BEC and other social engineering attacks. In a traditional BEC scam, hackers use a hacked or spoof email account belonging to an organization's leader to trick staff members into sending money to the hacker's bank account. Globally operating large organizations are a common target for BEC scammers.
- Business income lost as a result of an attack and other attack-related costs: Cybersecurity insurance policies may cover additional direct costs like forensic charges as well as lost business income. Policies may provide coverage for losses incurred by the insured business in the event of an attack on a third party, such as a partner or vendor. In light of the intricate supply chain ecosystem of today, this coverage is crucial.[11]
- Damaged reputation: Since many businesses depend on the confidence of their clients, experiencing a cyberattack can result in a temporary decline in sales. For a predetermined amount of time after a cybersecurity incident, damaged reputation coverage reimburses the insured for lost income due to reputational harm.

[10] Steven Bowcut, What is cybersecurity insurance and why do people need it, CYBERSECURITYGUIDE.ORG (Aug. 21, 2024, 10:04 AM), https://cybersecurityguide.org/resources/insurance/
[11] ibid

- Corporate Identity Theft: Losses brought on by unauthorized use of the business's digital identity may be covered. These offenses could take the shape of unlawfully signed contracts or credit that has been established fraudulently.
- Leadership Liability: Senior executives may be able to obtain coverage to shield them from legal action arising from a covered cyber event.[12]
- Cyber liability, also known as third-party insurance, can shield your company from lawsuits alleging damages from a cybersecurity incident. Attorney and court costs related to legal proceedings; settlements and court rulings; [13]and regulatory fines for noncompliance are typically covered by cyber liability coverage.

Liability of customers in case of Cybercrime related to Bank Transactions as per RBI

RBI has issued guidelines for figuring out a customer's liability in cybercrime situations.

- Zero Liability: In the first of the following two scenarios, a customer is not liable: Fraud, carelessness, or shortcoming on the bank's end, regardless of whether the transaction is reported or not.[14] A breach involving a third party occurs when there is no fault on the part of the bank or the customer. It is located elsewhere. The unauthorized transaction is reported by the customer to the bank.
- Limited Liability: Limited Liability: In a limited liability, the loss is the result of the customer's carelessness. Providing payment credentials, for example. Until the fraudulent transaction is reported to the bank, the customer is responsible for any losses.[15] The bank bears responsibility for the loss once it is reported. When another party, rather than the bank or the customer, bears the liability for the loss. The customer's transaction liability is capped at the transaction value in the event that the bank is not notified of the transaction promptly.

Indian scenario sifting from risk mitigation to risk prevention

Organizations that depend more and more on digitization to run their operations often use a variety of tactics to reduce the risks associated with cyberspace. Insurance vendors' or insurers'

---

[12] ibid

[13] Whitney Vandiver, Cybersecurity Insurance: What It Covers, Who Needs It, NERDWALLET (Aug. 21, 2024, 10:04 AM), https://www.nerdwallet.com/article/small-business/cybersecurity-insurance

[14] HDFC ERGO Team, 4 Types of Cyber Insurance Coverage in India You Should Know, HDFC ERGO, (Aug. 22, 2024, 11:08 AM) https://www.hdfcergo.com/blogs/cyber-insurance/types-of-cyber-insurance-coverages-in-india

[15] ibid

roles become crucial in assisting with these initiatives. Organizations are lagging in the implementation of cybersecurity measures due to the increase in sophisticated cyber threats. As per the Global Cybersecurity Outlook 2024 published by the World Economic Forum, there exist certain unsettling patterns that require attention. First, there is a growing disparity in cyber resilience across organizations; some have strong cybersecurity defences in place, while others are not ready[16]. According to a survey, almost 73% of the nation's mid-sized and large-sized organizations experienced a ransomware attack in 2023.[17] According to a survey conducted by cybersecurity firm Sophos, nearly 44% of these organizations had to pay a ransom between $100,000 and $500,000.[18]

According to the most recent data released by the National Crime Records Bureau (NCRB), India experienced a 24 per cent increase in cybercrimes registered in 2022 compared to 2021[19]. Other categories of crime, such as economic offences (11%), crimes against senior citizens (9%), and crimes against women (4%) also saw an increase.[20] As per the "Crime in India" report, there were 65,893 cases of cybercrime reported, which represents a 24.4% rise from the 52,974 cases in 2021[21]. "Under this category, the crime rate (per lakh population) rose from 3.9 in 2021 to 4.8 in 2022.

According to the report, the Indian cyber insurance market is currently estimated to be worth US$ 50–60 million and has grown at a consistent rate of 27–30 percent Compound Annual Growth Rate (CAGR) over the previous three years.[22] It is anticipated that this growth will continue for the next three to five years due to growing awareness of the importance of cyber insurance. Seventy percent of Chief Information Security Officers (CISOs) surveyed for the report indicated they would be willing to spend more money over the next three years to secure their digital infrastructure.[23] Remarkably, mid-sized businesses were the ones with the highest

[16] Himanshi Lohchab, Nearly 73% of Indian mid, large companies hit by ransomware in 2023, THE ECOOMIC TIMES, (Aug. 22, 2024, 11:08 AM) https://economictimes.indiatimes.com/tech/technology/nearly-73-of-indian-mid-large-companies-hit-by-ransomware-in-2023/articleshow/105518876.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
[17] ibid
[18] ibid
[19] Mahender Singh Manral, Jignasa Sinha, 24% rise in cybercrime in 2022, 11% surge in economic offences: NCRB report, THE INDIAN EXPRESS, (Aug. 22,2024, 11:08 AM) https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/
[20] ibid
[21] ibid
[22] Mou Chakravorty, Cyber insurance gains momentum in India; set to witness exponential growth: Deloitte's report, DELOITTE, (Aug. 22,2024, 11:08 AM) https://www2.deloitte.com/in/en/pages/financial-services/articles/cyber-insurance-gains-momentum-in-India.html
[23] ibid

willingness. On the other hand, some of the top consumer companies managing large consumer databases took a cautious approach when increasing their budgets for digital infrastructure. They did, however, indicate a desire to increase their insurance coverage. Approximately 60% of those surveyed desired more insurance coverage but were not willing to make significant investments in strengthening the security of their digital infrastructure.[24] According to the survey, there will likely be some short-term growth in the cyber insurance market, but momentum will likely lead to exponential acceleration.

Legislation related to Cybercrime and Insurance regulation in India

- **The Digital Personal Data Protection Act, 2023**

The Digital Personal Data Protection Act (DPDP) 2023, which attempts to control the way entities handle users' personal data, may incentivize businesses to get cyber insurance in order to reduce the risk of financial loss from liabilities. Section 33 of the act, which addresses penalties, is essential. It gives the data protection board the authority to fine data fiduciaries for failing to meet their obligations, especially when it comes to putting in place appropriate security measures.[25] Penalties could total up to Rs 250 crore[26]. It is also important to be aware of the potential additional responsibilities that could arise if any data fiduciary is designated as a Significant Data Fiduciary by the central government.[27] These responsibilities include a number of demands, including the hiring of an independent data auditor, designating a data protection officer, and carrying out regular audits and data protection impact assessments in addition to other regular audits[28]. Cyber insurance can assist organizations in meeting the requirements of the DPDP by providing the kinds of services covered in the preceding sections.

- **The Information Technology Act, 2000**

India's Information Technology Act of 2000 was the country's first significant cybersecurity law. The Indian Parliament passed the IT Act of 2000, which is managed by the Indian Computer Emergency Response Team (CERT-In). Its goals are to establish data protection guidelines, steer cybersecurity legislation, and control cybercrime. Among many other things,

---

[24] ibid
[25] The Digital Personal Data Protection Act, 2023, § 33, No. 22, Acts of Parliament, 2023 (India)
[26] The Digital Personal Data Protection Act, 2023, § 33, No. 22, Acts of Parliament, 2023 (India)
[27] The Digital Personal Data Protection Act, 2023, § 10, No. 22, Acts of Parliament, 2023 (India)
[28] Mr Rohit Kumar Sharma, Bridging Gaps in Cybersecurity with Cyber Insurance, INSTITUTE FOR DEFENCE STUDIES AND ANALYSES, (Aug. 21,2024, 10:04 AM) https://idsa.in/issuebrief/Bridging-Gaps-in-Cybersecurity-with-Cyber-Insurance-RSharma-210324

it safeguards e-banking, e-commerce, e-governance, and the private sector. Indian companies and organizations are required by Section 43A of the Act to have "reasonable security practices and procedures" in place to guard against the compromise, damage, exposure, or misuse of sensitive data.[29] Any intermediaries or individuals who divulge personal data without the owner's consent (with malice and causing damages) are subject to upto three years in prison and a fine of up to Rs500,000, or both.[30]

- **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**

The IT Act encompasses the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules), which constitute a significant component of cybersecurity legislation. The provisions pertaining to intermediary regulation, updated fines and penalties for cybercrime, defamation, cheating, and without consent publishing of private images, as well as speech restriction and censorship, are among the most important changes.[31] A person's right to update their information may also be granted by the regulations, which may also place limitations on data transfer, disclosure, and security precautions. They apply to corporate entities in order to safeguard sensitive personal data (SPD), which includes passwords, biometric data, medical history, and sexual orientation.[32]

- **National Cyber Security Policy, 2013**

To better safeguard public and private entities against cyberattacks, the Department of Electronics and Information Technology (DeitY) published the National Cyber Security Policy in 2013[33]. The National Cyber Security Policy seeks to improve the protection of India's cyber ecosystem by establishing more dynamic policies. Through skill development and training, the

[29] The Information Technology Act, 2000, § 43A, No. 21, Acts of Parliament, 2000 (India)
[30] The Information Technology Act, 2000, § 66, No. 21, Acts of Parliament, 2000 (India)
[31] Kyle Chin, op Cybersecurity Regulations in India, UPGAURD, (Aug. 21,2024, 10:04 AM) https://www.upguard.com/blog/cybersecurity-regulations-india
[32] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, INDIANKANOON, (Aug. 21,2024, 10:04 AM) https://indiankanoon.org/doc/114407484/
[33] Kyle Chin, op Cybersecurity Regulations in India, UPGAURD, (Aug. 21,2024, 10:04 AM) https://www.upguard.com/blog/cybersecurity-regulations-india

policy hopes to produce over 500,000 skilled IT professionals over the next five years.[34]

- **Reserve Bank of India notifications for Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs), 2018**

In 2018 notifications from the Reserve Bank of India outlining cybersecurity policies and procedures for Urban Cooperative banks. The 2018 RBI announcements seek to: establish uniform security frameworks across banks and payment providers based on their respective approaches to digitalization and new technologies.[35] Push banks to develop and submit their plans for managing cyber crises, direct banks to put into effect corporate-approved (board-approved) information security policies that effectively define cybersecurity readiness. Make banks submit required breach notifications, requiring UCBs to quickly identify and notify RBI of cybersecurity incidents within a few hours of discovery. Insist that banks plan frequent threat assessment audits. Support banks with Domain-based Message Authentication, Reporting and Conformance (DMARC) security controls and the implementation of anti-phishing and anti-malware technology on their own email domains.[36]

To address the growing business problems in a digital world and define frameworks for cybersecurity in payment processing, all Indian banks are required to adhere to these principles. Banks and the financial industry are subject to fines under the RBI notifications of 2018 for failing to comply with cybersecurity regulations.[37]

Regulating Authority for Cyber-crime and Insurance in India

- **National Critical Information Infrastructure Protection Center (NCIIPC)**

On January 16, 2014, the Indian government established the National Critical Information Infrastructure Protection Center (NCIIPC) in accordance with Section 70A of the IT Act, 2000 (as amended in 2008). [38]The NCIIPC, which has its headquarters in New Delhi, was designated

---

[34] National Cyber Security Policy, 2013, MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY, (Aug. 21,2024, 10:04 AM) https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf

[35] Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs), NOVOJURIS LEGAL, Aug. 21,2024, 10:04 AM) https://www.novojuris.com/thought-leadership/basic-cyber-security-framework-for-primary-urban-cooperative-banks-ucbs.html

[36] ibid

[37] Kyle Chin, op Cybersecurity Regulations in India, UPGAURD, (Aug. 21,2024, 10:04 AM) https://www.upguard.com/blog/cybersecurity-regulations-india

[38] About Us, NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE, (Aug. 21,2024, 10:04 AM) https://nciipc.gov.in/

as the country's primary contact for critical infrastructure protection. Furthermore, the NCIIPC is under the Prime Minister's Office (PMO) since it is considered a division of the National Technical Research Organization (NTRO).[39]

- **Computer Emergency Response Team- INDIA (CERT-In)**

CERT-In, the official name for the Computer Emergency Response Team, was established in 2004 as the country's central point of contact for gathering, evaluating, predicting, and sharing non-critical cybersecurity incidents.[40] The CERT-In cybersecurity directive aids in the issuance of guidelines for Indian organizations, providing the best information security practices for cybersecurity incidents in addition to reporting and notifying.

- **Cyber Regulations Appellate Tribunal (CRAT)**

The Cyber Regulations Appellate Tribunal (CRAT) was established by the Central Government of India under Section 48(1) of the Act,[41] with the primary responsibility for gathering information, receiving cyber evidence, and questioning witnesses. CRAT's jurisdiction for cybersecurity is limited in compare to that of CERT-In. CRAT have similar power as Civil court mentioned in Civil Procedure Code 1908.

- **Securities and Exchange Board of India (SEBI)**

The Ministry of Finance supervises the Securities and Exchange Board of India (SEBI), which was founded in 1988, as the regulatory body for the country's commodities and securities markets[42]. Because of the SEBI Act of January 1992, it has statutory authority and functions as an executive government body. SEBI makes sure that the requirements of investors, market intermediaries, and securities issuers are satisfied, including protecting their data, and digital transactions. Committee members appointed by SEBI as of April 2022 are mandated to supervise cybersecurity initiatives for the Indian market and advise SEBI on how to create and uphold cybersecurity regulations compliant with international industry standards.[43]

---

[39] Kyle Chin, op Cybersecurity Regulations in India, UPGAURD, (Aug. 21,2024, 10:04 AM) https://www.upguard.com/blog/cybersecurity-regulations-india

[40] About CERT-In, COMPUTER EMERGENCY RESPONSE TEAM, (Aug. 21,2024, 10:04 AM) https://www.cert-in.org.in/

[41] The Information Technology Act, 2000, § 43A, No. 21, Acts of Parliament, 2000 (India)

[42] What is SEBI?, BUSINESS STANDARD, (Aug. 21,2024, 10:04 AM) https://www.business-standard.com/about/what-is-sebi

[43] Advisory Committee for Leveraging Regulatory and Technology Solutions (ALeRTS), SEBI, (Aug. 22,2024, 10:04 PM) https://sebi.gov.in/sebiweb/about/AboutAction.do?doMember=yes&committeesId=64

- **Insurance Regulatory and Development Authority (IRDAI)**

IRDAI, which oversees the insurance industry in India, provides information security rules to insurers and emphasizes the significance of preserving data integrity and confidentiality. The first set of regulations, which addressed information and cybersecurity standards for insurers, was developed in 2017 by the Insurance Regulatory and Development Authority of India ("IRDAI").[44] The purpose of these rules is to guarantee that insurers possess adequate resources to handle any cyber-attack that may affect their data, systems, and procedures. The standards were expanded to cover all insurance intermediaries in 2022, which included web aggregators, brokers, corporate agents, third-party administrators (TPAs), and others.[45] Insurance businesses are required by the IRDAI to designate a chief information security officer, or CISO, in accordance with the new Information and Cyber Security for Insurers Guidelines (2023), establishes an information security committee, develops cybersecurity assurance programs, strategies for handling cyber crises, executes appropriate data protection techniques, and upholds risk identification and mitigation procedures.[46] Forms an information security committee, develops strategies for handling cyberattacks, designs and executes cybersecurity assurance plans, applies appropriate data protection techniques, and upholds risk assessment and mitigation procedures.

- **Telecom Regulatory Authority of India (TRAI) & Department of Telecommunications (DoT)**

Thus, on February 20, 1997, an Act of Parliament known as the Telecom Regulatory Authority of India Act, 1997, established the Telecom Regulatory Authority of India (TRAI) with the purpose of regulating telecom services, including the fixing or revision of tariffs for telecom services that were previously under the purview of the central government[47]. With effect from January 24, 2000, an ordinance amending the TRAI Act established the Telecommunications Dispute Settlement and Appellate Tribunal (TDSAT) to replace TRAI in its adjudicatory and dispute resolution roles. TDSAT was established to hear appeals against any TRAI directive, decision, or order as well as to decide disputes between a service provider and a group of

---

[44] NovoJuris Legal, An Overview of The IRDAI (Information And Cyber Security) Guidelines, 2023, MONDAQ (Aug. 22,2024, 10:04 PM) https://www.mondaq.com/india/security/1338148/an-overview-of-the-irdai-information-and-cyber-security-guidelines-2023#authors

[45] ibid

[46] ibid

[47] History of TRAI, TELECOM REGULATORY AUTHORITY OF INDIA, (Aug. 22,2024, 10:04 PM) https://trai.gov.in/about-us/history

consumers[48], between two or more service providers, and between a licensor and a licensee. The Department of Telecommunication (DoT) and the Telecom Regulatory Authority of India have strengthened rules regarding user data privacy and usage. In India, the Ministry of Communications has a separate executive department called DoT and a regulatory body called TRAI. Together, TRAI and other regulatory agencies oversee and regulate telephone operators and service providers, despite TRAI having more regulatory authority.

Challenges in respect of effectiveness of Cybersecurity Insurance

Institutional investors find it difficult to model cyber risk because, in contrast to traditional insurance, cyber risk insurance is a relatively new idea and there is a lack of data on cyber incidents. It is more challenging for insurers and the insured to stay up to date with emerging threats due to the swift changes in the threat landscape. For example, in February 2024, it was reported that a financial employee fell for a scam employing deepfake technology, which resulted in the paying fraudsters $25 million.[49] It will be interesting to observe how the insurance sector responds to these threats created by artificial intelligence and what kind of coverage it offers.The lack of data, coupled with the threats posed by emerging technologies, instils ambiguity among insurers, leading to reluctance to cover risks that appear to be too risky to share. This unwillingness is more profound in the case of state-sponsored cyber-attacks and terrorism, often resulting in exclusion clauses that specifically exclude coverage for losses stemming from such acts.[50] Payments for cyber extortion, particularly ransomware, pose a contentious dilemma for organisations. On one hand, paying ransom can facilitate the recovery of data. However, on the other hand, it also effectively contributes to fuelling a criminal ecosystem, potential incentivising perpetrators to carry out similar attacks in the future.

Insurers become uncertain due to a lack of data and the threats posed by emerging technologies, which makes them reluctant to cover risks that seem too risky to disclose.[51] In the event of state-sponsored cyberattacks and terrorism, this reluctance is more prominent and frequently leads to exclusion clauses that expressly deny coverage for losses resulting from such actions.

---

[48] ibid

[49] Mr Rohit Kumar Sharma, Bridging Gaps in Cybersecurity with Cyber Insurance, INSTITUTE FOR DEFENCE STUDIES AND ANALYSES, (Aug. 21,2024, 10:04 AM) https://idsa.in/issuebrief/Bridging-Gaps-in-Cybersecurity-with-Cyber-Insurance-RSharma-210324

[50] ibid

[51] Alex Zukerman, 8 Cyber Insurance Challenges, SAPIENS, (Aug. 24,2024, 10:04 AM) https://sapiens.com/blog/8-cyber-insurance-challenges/#:~:text=8%20Cyber%20Insurance%20Challenges%201%20Lack%20of%20Historical,Geographical%20Limitation%20...%207%20The%20Actuarial%20Paradox%20

For organizations, payments for ransomware, in particular, present a difficult problem. Compared to traditional coverage, the geographic scope of cyber insurance coverage is far more ambiguous. Physical geographical boundaries mean nothing to cyber attackers, who, once inside the system, can operate freely from any location within the organization's premises.[52] It is challenging for organizations to determine the appropriate policies and recommendations regarding data privacy and cybersecurity from vague laws and disjointed legislative approaches.

Conclusion

The increasing prevalence and severity of cybercrime can be attributed to factors such as globalization, digitization, and smart technologies. Even though this is a relatively young field of research and business, having robust cybersecurity defensive measures is essential. At the corporate, national, and international levels, this has been observed. Cybersecurity insurance protects businesses against a range of financial losses, such as theft, ransomware payments, data breaches, and system hacking. Underwriters find it difficult to estimate cyber risk since, in contrast to traditional insurance, cyber risk insurance is a relatively new idea and there is a lack of data on cyber occurrences. It is more challenging for insurers and the insured to stay up to date with developing hazards due to the swift changes in the threat landscape. It will be interesting to observe how the insurance sector responds to these concerns created by artificial intelligence and what kind of coverage it offers.

[52] ibid