International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2025 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Cyber Insurance & Legal Challenges in the Age of Digital Risk

Alina Raza[a]

[a]SOA National Institute of Law, Bhubaneshwar, India

Received 01 November 2025; Accepted 02 December 2025; Published 06 December 2025

The rapid expansion of digital technologies has transformed global economic and institutional systems while simultaneously amplifying exposure to sophisticated cyber risks. Escalating incidents such as ransomware, supply-chain intrusions, data breaches and emerging AI-enabled attacks have compelled organisations to reassess traditional security models. Cyber insurance has consequently evolved as a critical risk-transfer mechanism, offering financial protection, incident-response support, and regulatory compliance assistance. This paper examines the conceptual foundations, evolution and significance of cyber insurance, with emphasis on its growing relevance in the digital economy. It analyses contemporary cyber-threat landscapes, major insurance coverage models, and jurisdictional approaches in the United States, European Union and India. Further, it explores key legal challenges including attribution complexities, regulatory ambiguities, cross-border data-governance issues, and the lack of standardised policy wording. The study concludes that while cyber insurance strengthens organisational resilience, its effectiveness depends on harmonised legal frameworks, improved risk-assessment tools and continuous adaptation to emerging cyber threats.

Keywords: *cyber insurance, digital risk, legal challenges.*

INTRODUCTION

In the modern hyperconnected world, digital technologies are an essential building block of modern economies, businesses and societies. Whether we are talking about financial transactions or healthcare systems, e-commerce platforms, or critical infrastructure, virtually all kinds of modern life are digitalised. The digital revolution has enhanced globalisation and convenience on an unparalleled scale; however, it has also given rise to cyber risks that endanger the functioning of individuals, businesses, and governments.

Hacking, data breaches, ransomware, cyber identity theft, and online fraud are not one-off events any more but common problems that can result in substantial monetary loss as well as reputational and national security crises. The damage done to finances and reputation as a result of such incidents has put cyber insurance as a growing and important tool of risk management. Contrary to the classical insurance policies, cyber insurance is specific as it is meant to cover intangible but also devastating damages of digital assets, networks and protection of their data. The most efficient risk management tools have been ineffective in tackling these forms of unwanted risks, which continue to multiply in number and sophistication as cyber wars rage on.

Cyber insurance is a form of coverage that is based on reducing the monetary and operational repercussions of cyber-related incidents. Besides a monetary cover, cyber insurance includes assistance in the event of an incident, defence in case of legal proceedings, forensic analysis and help with compliance with the data protection regulations. Nevertheless, the emergence of cyber insurance is still in its infancy stage and it faces problems that are not readily available in traditional insurance programs, such as risk definition, premium establishment, and liability.

Meanwhile, the legal and regulatory environment of digital risks is continuously changing. Matters of cross-border transfer, privacy, jurisdiction on cybercrimes, contracts and adherence to data protection laws (e.g. the GDPR in Europe or the Digital Personal Data Protection Act, 2023[1] in India) present intricate legal barriers to both insurers and policyholders.

The dynamic nature of cyber insurance makes it distinct from traditional insurance, which typically addresses only specific risks and their applicability. Furthermore, existing legal

[1] Digital Personal Data Protection Act 2023

frameworks remain fragmented, as they attempt to address issues such as attributing cyberattacks, determining liability, enforcing cross-border data protection policies, and ensuring compliance with evolving cybersecurity regulations. Such multidimensional issues make it difficult not only to draft and interpret the insurance contracts but also to enforce them in jurisdictions with varying statutory and regulatory frameworks. As such, it is not a coincidence that cyber insurance and its legal concerns have to be studied, but an absolute necessity of the modern digital landscape.

It goes into a discussion of the ways in which societies can become resilient to cyber risk, how to strike a balance between technological development and legal protections and how to make the digital economy a trust-based environment. The subject matter is of particular importance due to the increased attempts of the business, governments, and individuals to find dependable ways to mitigate cyber risks and manage the complex legal frameworks implemented in the sphere of digital security. In this regard, it will be necessary to explore the interrelation between cyber insurance and the law, as it can help to realise how the communities can build robust frameworks related to addressing the twenty-first-century digital risks.

In this respect, this paper positions cyber insurance as both a risk management tool and a legal field of study with its major changes and shifts generated by the critical issues in response to liability, accountability, and a relevant regulatory aspect of cyberspace.

MEANING AND EVOLUTION OF CYBER INSURANCE

Meaning: Cyber risk insurance, also referred to as cyber risk insurance and cyber insurance, is a type of speciality insurance that covers businesses against the risk of cyberattack and other cyber threats. It offers coverage to expenses incurred as a result of data breaches, ransomware attacks, system downtimes and other cyber-related disruptions. Cyber insurance is unlike traditional insurance as it specifically covers the perils associated with cyberspace, such as potential liabilities created by data privacy laws, claims brought against by third parties, and the general costs of incident response. The legal experts have given broad definitions of cyber insurance in recent years.

Legal scholars have provided comprehensive definitions of cyber insurance in recent years. According to Josephine Wolff, “Cyber insurance is a financial instrument for transferring some

of the costs and risks of cybersecurity incidents to an insurer, in exchange for a premium." Similarly, Woods and Simpson define it as: "Cyber insurance refers to contracts designed to protect organisations against losses arising from information security breaches, data theft, and related cyber incidents."[2]

Both of the definitions confirm that cyber insurance is a risk-minimisation instrument that enables companies and individuals to be safe against increased costs and liability risks of cyberattacks. In the modern world of the digital economy, where risks of any concentrated form act as a significant factor in comprehensive risk management strategies, it plays a significant role.

EVOLUTION

Global Evolution of Cyber Insurance –

Early Years (1990s to early 2000s): The idea of cyber insurance came into existence essentially in the late 1990s when it became apparent to insurance companies that businesses were becoming heavily dependent on digitalisation and an internet connection. AIG was the first company to offer a cyber insurance policy in 1997.[3] Originally, these offerings were few and were to cover risks like data loss, liability to hacking, and errors and omissions due to technology services. But the coverage was minimal and usually supplementary to broader liability policies.

Growth with Rising Cyber Threats and Regulation (mid-2000s to 2010s): The market has grown due to issues with cyberattacks like data breaches and denial-of-service attacks, as they happen more often and have increased sophistication. Responses through rules to protect the personal information of consumers were developed, and governments came into action with the California Consumer Privacy Act and later the GDPR in the EU. These policies caused companies to enhance their cybersecurity framework and introduced the market to demand insurance that will offset the penalties imposed by law, legal defence costs, and notification costs in the event of a breach. Meanwhile, cyber-insurance had moved to cover more and more

[2] David W Woods & Andrew Simpson, 'Policy measures and cyber insurance: a framework' (2017) 2(1) Journal of Cyber Policy <https://doi.org/10.1080/23738871.2017.1360927> accessed 25 October 2025
[3] Rachael King, 'Health-Care Industry Starts to Pay Attention to Cyber Risks' The Wall Street Journal (07 November 2014) <https://www.wsj.com/articles/BL-CIOB-5729> accessed 25 October 2025

sophisticated types of loss (business interruption, extortion, forensic investigation), as well as a third-party liability line of defence (lawsuits, regulatory investigations). There was also an improvement in pricing models, as well as in underwriting processes, and the collection of more claims data by the insurers.

The Actual Days (2020s and onwards): The past five years have witnessed the growth and development of the market. The risk of cybersecurity was increasing with the rise of ransomware, supply chain activity, as well as nation-state hacking, making these happenings to an increase. In the meantime, the cost of cyber insurance coverage had escalated, as cyber insurance coverage had widened, and businesses were more vulnerable to the loss of their data.

Recent Trends and Current Market (2020s and beyond): The past five years have been associated with rapid growth and maturity of the market. The emergence of ransomware, supply chain and nation-state hacking raised the risks to cybersecurity worldwide. Meanwhile, premiums on cyber insurance increased and premiums on policies with broader coverage grew. The leading market currently is the U.S., with nearly 70 per cent of total cyber insurance premiums worldwide, and the European and Asia/Oceania markets are expanding rapidly.[4] Insurers have recently started to demand insureds exhibit excellent cybersecurity protocols as a prerequisite to coverage. New instruments like artificial intelligence and machine learning are among the technologies and analytics that are being implemented to enrich underwriting and risk management. The cyber insurance industry is forecasted to expand rapidly, reaching over $20 billion in premiums by 2025 and possibly $40 billion by 2030, due to increasing cyber threats and greater awareness.

EVOLUTION OF CYBER INSURANCE IN INDIA

Initial Phase (Pre-2014): In India, the insurance industry did not evolve, as observed in Western societies, in the early years, in terms of cybersecurity. Until recently, cyber risks were generally combined with other coverages, e.g. professional indemnity covers or property policies, and they were not offered as single coverage. It was identified that there was limited awareness and understanding of cyber insurance among Indian businesses.

[4] AM Best, *Cyber Insurance Market Report* (2022)

Market Emergence (2014-2018): Cyber insurance policies became increasingly common in 2014, with a tendency to target IT companies, large companies, and banks subject to international regulations, including GDPR. The level of adoption was low, and poor growth was recorded as companies faced difficulties in interpreting the policy and also in assessing exposure. The early adoption level was higher amongst FSI businesses and the IT sector, as these operations were data and regulatory-intensive.

Speedy Adaptation and Development (2018 Onwards): Demand has been accelerated by a variety of factors, as the Indian start-ups turned more digitalised, posing greater threats in their cyber risk exposures, necessitating that a formal risk management tool is in place. There was the prospect of increased regulatory frameworks on personal data protection in India and more stringent cybersecurity requirements by the RBI, which acted as an incentive to insurance buying. The reasons Indian business owners are losing their sleep include the possibility of monetary and brand leverage associated with the leakage of Aadhaar information and ransomware attacks on businesses. The manufacturing sector, the healthcare sector, Retailing and startups and individuals have been on a buying spree of cyber insurance as they are increasingly relying on digital dependence.

Data on market size indicate that the premium pool in India has increased to about $500 million in 2024, compared to around $10 million in the year 2014, with future projections to reach above 6.9 billion at a CAGR of nearly 29%.[5]

IMPORTANCE OF CYBER INSURANCE IN THE DIGITAL ECONOMY

Cyber insurance, on the other hand, is an insurance service that offers financial coverage against loss realised due to cyber-attacks and data breaches, which includes data recovery expenses, legal liability, and business interruption. Its importance to the digital economy cannot be overestimated because it is necessary to secure resilience in operations, build trust among consumers, and streamline regulatory compliance.

[5] Karl Hersch et al., '2024 global insurance outlook' (*Deloitte*, 28 eptember 2023) <https://www.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-outlooks/insurance-industry-outlook-2024.html> accessed 25 October 2025

Business Continuity: Cyberattacks have the potential to cripple the business of an organisation, resulting in loss of revenue, extended system downtime, and extra recovery costs. By providing various advantages, cyber insurance guarantees operational resilience.

Liability Coverage: Cyber incidents can result in an accumulation of expenses in the form of system network costs, data-restoration expenditures, IT forensics, litigation, and even customer notification. When insurance is not obtained, these costs can severely jeopardise the financial viability of a company. Cyber insurance can reduce this burden so that organisations can also recover.

Crisis Management and Incident Response: Leading insurers provide access to specialised services such as digital forensic investigations, regulatory breach notifications, and media management. These services enable organisations to address the immediate consequences of a cyberattack and restore normal business operations swiftly.

Business Interruption Coverage: Longer periods without operation may damage supply chains, lead to delays in delivery, and cause a considerable loss of customer confidence. Cyber insurance coverages can include coverage of loss of income during recovery time so that an organisation may be in a position to maintain stability.

Recent statistics justify why this should be done urgently. The IBM Cost of a Data Breach Report 2023 revealed an average cost of a data breach of USD 4.45 million, a 15 per cent increase in 3 years.[6] The expensive cost environment has made cyber insurance an important part of corporate risk management strategies.

Consumer Trust and Compliance: Consumer trust is an essential asset in this era of the digital economy. Cybersecurity considerations, such as robustness and preparedness of contingencies, are expected of businesses by customers.

Cyber insurance enhances this trust and makes compliance in several ways –

[6] IBM Security, *Cost of a Data Breach Report 2023* (2023)

Data Protection Assurance: Using computer insurance gives the company a sign to the consumers that the company is keen on protecting information. This helps to earn the trust and will discourage people from leaving after an event of breach.

Regulatory Compliance: The global and national data privacy regulations come with huge compliance requirements for businesses. One example is the GDPR of the European Union, which has strict data processing and breach notification requirements.[7] Equally important, the Digital Personal Data Protection Act of India, 2023, requires express consent and imposes fines when there is non-compliance.[8] Cyber insurance can assist companies with these requirements to meet legal costs and penalties, as well as make breach notifications in a timely manner.

Reputation Management: Besides the reality of direct financial loss, there is a loss of brand reputation and customer loyalty associated with data breaches. A lot of cyber insurance policies cover costs relating to publicity and brand recovery efforts, which allows businesses to recover trust after the occurrence of an event.

Risk Transfer and Financial Protection: Cyber risks also do not stay as they are because they are dependent on advancing technology and new and smarter techniques of attack. The absolute prevention is almost impossible, even with the greatest cybersecurity precautions. Cyber insurance is a risk transfer system that helps to transfer part of the economic responsibility to the provider. Such a mechanism is particularly important to small and medium-sized enterprises (SMEs) that usually do not have their own cybersecurity specialists or reserves. In the absence of insurance, a one-time ransomware attack can render SMEs into bankruptcies. Cyber insurance also spreads risk and allows such entities to endure the effects of a disaster that would otherwise spell doom to them.

Enabling Digital Innovation: The entry of new types of technologies, such as cloud computing, AI, and IoT, into the business sphere of interest makes many companies reluctant to adopt them because of the cybersecurity threat. Although such technologies bring efficiency, they increase the battlefront area of the malicious actors. The presence of cyber insurance can be seen as a security net, and this helps companies implement digital transformation plans without

[7] General Data Protection Regulation 2016
[8] Digital Personal Data Protection Act 2023

worrying too much about the possibility of a substantial financial loss. In effect, it promotes innovation where technological progress is balanced with risk control.

Investor and Stakeholder Confidence: Cybersecurity has become a fundamental business governance issue that drives stock-market decisions and investor morale. Institutional investors are progressively looking to see evidence of well-developed cyber-risk management programs, and as such, may view such coverage as a good sign. Firms with effective products in cyber insurance will communicate effectively that they are strong and prepared for incoming threats, thus gaining credibility and favour with investors. Indeed, one PwC report notes that companies experienced improved access to capital and slighter higher valuations when management exhibited visible cyber-risk strategies such as insurance. In fact, according to one PwC report, firms with visible cyber-risk strategies, such as insurance, have better access to capital and higher valuations.[9]

CURRENT CYBERSECURITY THREATS AND TRENDS AS INSURANCE DRIVERS

In the current section, we introduce prevailing cyber risks that, as research reveals, are causing difficulties to organisations, and this prompts them to search out cyber insurance cover, such as supply-chain attacks, ransomware, business email compromise and funds transfer fraud.

Ransomware: Ransomware can be summed up as a malicious attack where the attackers encrypt the data of an organisation and demand payment (ransom) to unlock the data. Ransomware has been evaluated and ranked as the top risk during 2020-2021, with a number of high-profile and widely reported falls. Ransomware has advanced to the point of so-called double extortion, where the criminals blackmail their targets not only to restore the encrypted database but also threaten to publish the data in a third-party medium. According to the researchers and reports, there is an ever-increasing ransomware attacks per month in 2020 and 2021.[10] Along with the rising frequency of ransomware attacks, it has also been observed that the ransom amount demanded continues to rise as well.

Supply Chain Attack: A supply chain attack is a form of a cybersecurity threat in which attackers can gain illicit access to an organisation by hacking its suppliers, service providers or

[9] PwC, *Global Digital Trust Insights 2024* (2024)
[10] *ENISA Threat Landscape 2021* (October 2021)

third-party vendors. Other than attacking the primary target itself, hackers use the supply chain trust relationship to gain access through malicious software updates, hardware components or any third-party access credentials.

One of the most destructive forms of attack is that it can impact multiple organisations at a time, as was the case in 2020, the SolarWinds Orion hack impacted numerous U.S. government agencies along with major companies, and in the Target breach (2013), where the attackers used a vendor to gain access to the payment systems.[11] Attacks on the supply chain are hard to identify and remediate since they are launched by trusted third parties and spread undetected.

The growing adoption of such measures has major implications for risk management and regulatory compliance, particularly under frameworks like the GDPR and India's Digital Personal Data Protection Act, 2023, which hold companies accountable for data breaches caused by third parties. This has made cyberattacks a leading catalyst behind cyber insurance policies, which cover third-party liability and vendor-related risks.

Business Email Compromise: Business email compromise (BEC) refers to an attack where the attacker manages to gain control over the email account of an employee and uses such privileges to take other actions that are unauthorised (e.g., impersonating an authorised party). In such a way, BEC can ultimately result in various losses, such as ransomware, funds transfer fraud, and data breaches, among others. To indicate the implications of BEC attacks, it is documented that the expense of BEC attacks in the United States in 2019 was about 1.7 billion dollars, and the average cost of BEC attacks in 2020 and 2021 was 30 thousand dollars and 50 thousand dollars, respectively.[12]

A large increase compared to 2020, BEC attacks spread more widely across industries and regions in 2021. The circumstances that were created during the COVID-19 pandemic helped the rise in BEC incidents, since face-to-face interactions and in-person communication were diminished, often due to replacing them with email-based communication.

[11] *The Radicati Group*, *Advanced Persistent Threat (APT) Protection- Market Quadrant 2023* (March 2023)
[12] IC3, *Internet Crime Report* (2019)

Phishing and Social Engineering: Phishing and social engineering are among the most popular and enduring types of cyberattacks, and they are leaning on human weaknesses instead of technical vulnerabilities. Phishing attacks involve faking the identity of an established, trusted organisation, like a bank, government or a contractor executive, to get people to divulge private information, often passwords or financial details.

Social engineering is more than just phishing emails and may be done over the phone or by text message, or even face-to-face in order to trick victims into giving up access to secure systems. Recent examples, like the 2020 Twitter breach, in which attackers social engineered their way into employee credential access and took over celebrity accounts, demonstrate the drastic impact of such attacks.

Phishing and social engineering are especially threatening because they break through even the most advanced technical protection methods by producing vulnerability at the least secure point in human behaviour. Regulatory-wise, the implementation of thorough awareness and training programs to prevent these risks have become a requirement by data protection laws such as the GDPR in Europe or the Digital Personal Data Protection Act, 2023, in India.[13]

Fraud in Funds Transfer: Funds transfer fraud (FTF) is are breaches that seek to exploit authorised users or activities to wire funds to a recipient that should not receive the funds. As a rule, FTF is executed after other attacks, in particular, after ransomware or social engineering. Other, more complicated attacks, like ransomware, demand the use of more sophisticated methods, tools and knowledge. FTF is commonly carried out using BEC and social engineering, hence it is simpler to execute. Total losses, however, can be considerable; in 2021, on average, 326 thousand dollars were lost per FTF attack, which is a rather large figure compared to the previous year, 124 thousand dollars.[14]

Denial-of-Service and Distributed Denial-of-Service: Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are cyber threats striving to interrupt the normal process of the target server, network, or service. In a DoS attack, an entire system is blocked by a single computer to slow it down or crash so that it cannot be accessed by genuine users. A DDoS attack is even more serious in that it employs multiple compromised hosts, typically in a botnet,

[13] General Data Protection Regulation 2016; Digital Personal Data Protection Act 2023
[14] Coalition, *Cyber Insurance Claims Report* (2021)

to bombard the victim with traffic at once. Such attacks have the capabilities to cripple business and even lead to financial losses and a tarnished name. They are often used not only to cause any disruption but also as a staging ground to hide other criminal activity, like a data breach or a network intrusion.

Insider Threats: This is a category of cyber risks caused by people who are part of an organisation because they intentionally or unintentionally violate security. Malicious insiders can purposely steal sensitive information, damage systems, or even assist in an outside attack in order to receive personal benefits or financial gain or as retaliation against the employer. On the other hand, irresponsible insiders are the ones who cause systems to be endangered due to inconsiderate actions, which include poor password habits, becoming victims of phishing, or mismanaging sensitive information. Insiders already possess valid access to organisational resources, so the detection and prevention of such threats is especially problematic. Insider threats may result in serious outcomes such as loss of finances, regulatory fines, reputational damages or even hindered operations, thus being amongst the most complicated risks to manage as far as cybersecurity is concerned.

Cloud and Virtualisation Risks: Risks of Cloud and Virtualisation occur due to the escalating reliance on cloud technologies and virtualised networks for storing and processing data. Among such risks, there is the potential exposure of sensitive data to unauthorised access due to misconfigured cloud storage and weak identity and access management controls that can be used by attackers to exploit accounts. The tendency to have shared responsibility between cloud providers and customers will cause security gaps since each party will believe that the other party is taking care of certain protection. The added complexity related to virtualisation is that breaches in the hypervisor or virtual machines can offer an avenue of access to attackers who can use this avenue to breach several systems. Such risks may lead to data loss, service downtimes, and regulatory violations, making sure that security setups and monitoring are well covered in the cloud environment.[15]

[15] Wayne Jansen and Tim Grance, 'Guidelines on Security and Privacy in Public Cloud Computing' (*NIST*, December 2011) <https://csrc.nist.gov/pubs/sp/800/144/final> accessed 25 October 2025

IoT and Smart Device Risks: These are the vulnerabilities that arise due to the spread of devices connected to the Internet of Things (IoT), smart appliances, apparel and devices, industrial sensors and connected automobiles. Those devices are less likely to possess robust security measures, weak or default passwords, and are not regularly updated with new firmware, providing cybercriminals with the incentive to exploit them.

When breached, IoT devices might become stepping stones to larger networks, or their use as a springboard to become deployed in vast botnets attacking major global systems as DDoS operations. Moreover, the IoT devices are often used to gather sensitive personal or organisational data, the loss of which will result in the breach of privacy and, subsequently, regulatory non-compliance. IoT ecosystems are so complex and large that they exacerbate the difficulty of securing them and call for formidable encryption, network segregation, as well as subsequent monitoring.

EMERGING RISKS IN CYBER SECURITY

AI-powered Attacks: AI-associated Attacks use artificial intelligence to develop convincingly spoofed phishing emails, develop evasive malware, and global fake content to perform fraud or misinformation campaigns. These attacks are more difficult to detect because of the level of automation and precision of the attack.

Cryptojacking: Cryptojacking happens when attackers secretly use someone's computer power, like CPUs or GPUs, to mine cryptocurrency. They usually spread malware or take advantage of software weaknesses, which slows down systems and raises costs for victims.

Quantum Computing Threats: The risk posed by quantum computing is largely hypothetical at least, but has the potential to be a serious threat down the line since quantum algorithms have the capability of cracking commonly-used cryptography protocols, such as RSA and ECC, making any encryption broken by such an event obsolete. Such risks make it necessary to investigate the potential of cryptographic solutions that are quantum-resistant in order to protect data in the post-quantum world.

SCOPE OF CYBER INSURANCE POLICIES

Cyber insurance policy scope describes the extent and boundary of the protection proposed to the insured. It consists of the parties added, the events that are covered, the expenses that can be covered by the insurance and the Jurisdiction or territorial sphere covered.

Who is Covered?

Cyber insurance policies are mainly intended to cover business organisations, irrespective of their size, be it a small set-up or multinational companies, to government agencies dealing with critical infrastructures and sensitive information. Several insurers have specialised products available to individuals, especially in relation to identity theft protection and protection against the breach of personal data. The policyholder is the insured party, the stakeholder who would generally lock up or work with data and is legally or contractually obliged to protect the data.

What Events are Covered?

This scope consists of a broad set of cyber-related events, risks, and breaches, like malicious cyberattacks, data breaches, denial-of-service (DoS) attacks, ransomware, insider threats, phishing, and privacy infractions. As an illustration, when an organisation becomes a victim of ransomware attacks, which lock its data and accompanies it with a payment of ransom, the policy usually covers the costs of negotiations with the attackers and restoring the system.[16] In the same manner, unauthorised access or disclosure of personal information, using which potential liability arises in the form of privacy liability and regulatory penalties, is covered.

What Costs are Covered?

Indirect costs are likely to be covered by cyber insurance. Direct Costs can consist of data restoration, repair of the system, forensic investigation, breach notification, and customer credit monitoring. Indirect Costs involve the business interruption loss, fines incurred by the business regulatory bodies (where legally insurable) and reputation management costs. Adopting this two-fold strategy can ensure businesses not only overcome the short-term technological

[16] '2022 Marsh and Microsoft global cyber risk survey' (*Marsh*) <https://www.marsh.com/en/services/cyber-risk/insights/global-cyber-risk-survey.html> accessed 25 October 2025

repercussions of an incident, but can also ensure that they overcome the longer-term financial and reputational impacts of the incident.

Jurisdictional Scope: The majority of cyber insurance policies do have worldwide coverage due to the fact that cyber breaches can occur across borders. Nevertheless, the insured must adhere to the existing data protection and cybersecurity rules, including the General Data Protection Regulation (GDPR) in the European Union or the Digital Personal Data Protection Act, 2023, in India.[17] Failure to comply with such laws might entail regulatory costs that might not be included in full, and possibly not at all, in the coverage, owing to local regulations that might not allow them to be so insurable.

TYPES OF CYBER INSURANCE POLICIES AND COVERAGE

Cyber insurance policies are primarily designed to cover various types of risks and liabilities posed by cyber incidents. Generally, these policies fall under two categories, and they include the First-Party Coverage and the Third-Party Liability Coverage. Moreover, many insurers do provide specialised or hybrid policies to serve some unique industry needs.

First-Party Coverage: Unlike Third-Party Coverage, which covers losses incurred by third parties, First-Party Coverage covers losses sustained by the affected organisation itself as an outcome of the cyber incident. Between costs incurred to address the internal impact of a cyber event and costs incurred to recover, this type of coverage covers costs.

Major Highlights of First-Party Coverage are –

Data Breach Response Costs: Coverage provides forensic investigation, notification costs of breach and monitoring of the credit of affected individuals.

Data Restoration and System Repair: This is the coverage of costs that are involved in restoring or replacing corrupted data and repairing affected systems.

Business Interruption Losses: Covers the loss of income and additional costs spent on system unavailability or interruptions of operational processes induced by the cyberattack.[18]

[17] General Data Protection Regulation 2016; The Digital Personal Data Protection Act 2023
[18] NAIC, *Cybersecurity Insurance Coverage* (2023)

Cyber Extortion (Ransomware): Covers expenses associated with ransom negotiations, ransom payments, and hiring of cybersecurity consultants in response to ransomware incidents.

Crisis Management, Reputation Management: The costs of publicity and crisis communication measures aimed at reducing reputational losses as a result of a cyber incident.

Third-Party Liability Coverage: Third-Party Coverage covers the insured against claims made by third parties due to a breach of data security or lack of conformity with privacy laws.

The Key Issues of the Third-Party Coverage are –

Privacy Liability: Court fees and payments in some cases, and settlements associated with illegal compromise of personal or confidential data.

Network Security Liability: The claims that can arise due to personal failure to prevent cases of cyberattacks include cases of malware transmission or denial of service, which affect a third party.

Regulatory Fines and Penalties: Penalties and Fines by the Regulators Coverage penalties imposed within the scope of data protection laws, where such coverage is provided by legally accepted insurance (e.g., GDPR, DPDP Act).

Media Liability: Shielding against a charge of defamation, copyright infringement or violation of the intellectual property relating to digital content.

Specialised Policies and Hybrid Policies: Cyber insurers increasingly design industry-specific policies that reflect the unique risk exposures of different sectors. For instance, healthcare organisations require greater protection against breaches related to HIPAA compliance, while financial institutions need broader coverage for payment fraud and regulatory liabilities. Similarly, technology service providers and software firms often combine cyber insurance with technology errors and omissions (E&O) policies, creating a more comprehensive framework to address both cyber risks and professional liability.

GLOBAL PERSPECTIVE OF CYBER INSURANCE

Cyber Insurance in the United States: In the global cyber insurance market, the United States enjoys a commanding position and accounts for an overwhelming share of about 59% of all premiums globally. The U.S. cyber insurance industry is relatively new and was approximately USD 810 billion in 2024; however, the market is anticipated to expand significantly in the coming years due to several factors. A key driver of this growth is the increasing frequency and severity of ransomware attacks, which disrupt business operations, encrypt critical data, and involve extortion demands for substantial payments. As a result, companies are finding it necessary to take cyber insurance to cushion themselves against these losses.

Regulatory requirements have also increased, making organisations tighten up their cybersecurity policies and secure an incident report within a set time. Specifically, there are federal and state anti-hacking laws, and industry-specific regulations whose requirements are quite high in terms of breach notification, thus contributing to the overall costs of a cyber incident. The other reason that has led to the increased demand for cyber insurance is the increased trend of class-action lawsuits, which occur after data breaches. This increased legal vulnerability has seen companies act to transfer risk with the comprehensive cyber insurance policy available both to cover the financial implications of the loss, as well as legal advice and incident response services.

Legal and Regulatory Framework –

The U.S. lacks a single major federal privacy law, as does the GDPR-driven approach in the EU. We have, instead, a quilt of state and federal laws that actually influence the cyber insurance market.

State-Level Privacy Laws: The Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), grant consumers extensive rights and impose mandatory breach notification requirements, which in turn influence insurance coverage for regulatory fines and legal defence. Similar rules have been adopted in a bunch of other states (e.g., Colorado, Virginia, Utah, Connecticut).

Federal Sector-Specific Laws: The healthcare industry is within the confines of HIPAA. And GLBA regulates financial institutions.

Breach Notification Laws: Each of the 50 states will now have to inform people (and even regulators) in case a breach takes place. That drives incident response and crisis-management cover demand.

Cybersecurity Regulations for Specific Industries: The Department of Financial Services (NYDFS) of New York has the Cybersecurity Regulation (23 NYCRR 500), which requires financial companies to operate cyber programs, report, and certify that they are in compliance.[19] The FTC Safeguards Rule extends to Non-bank financial institutions, including breach reporting (effective May 13, 2024).[20]

SEC Cybersecurity Disclosure Rules: The new rules that were put in place by the Securities and Exchange Commission (SEC) in December 2023 include the following: Publicly listed companies must disclose material cyber incidents by filing Form 8-K within four business days of determining their significance. Additionally, Form 10-K requires annual reporting on cyber governance, including risk management practices, strategic measures, and board oversight. These regulations raise the exposure of Directors and Officers (D&O) liability, and an increasing number of firms demand cyber policies that provide regulatory investigation coverage, which places an extra burden on the underwriting diligence.

Cyber Insurance in the European Union: The European Union (EU) has emerged as one of the fastest-growing cyber insurance markets, driven largely by the stringent data protection framework introduced through the General Data Protection Regulation (GDPR), effective from May 25, 2018. Compared to the U.S., where the legal environment is relatively fragmented, the EU imposes a homogenous, harmonised approach to data privacy, leaving companies operating in its territory with a set of obligations in the event they process the personal data of EU residents.

---

[19] 'CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES' (*DEPARTMENT OF FINANCIAL SERVICES*) <https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf> accessed 25 October 2025

[20] The Code of Federal Regulation, pt 314

The penetration rates in countries such as the United Kingdom, Germany, and France are higher, owing to the fact that they have developed digital infrastructure and actively enforced their regulatory measures. Smaller economies and smaller firms, in turn, tend to remain underinsured due to cost reasons and a failure to be aware of cyber risks. Nevertheless, the general direction here is unmistakable, as regulatory scrutiny increases with the GDPR, an increasing number of organisations are considering cyber insurance as an important component of enterprise risk management.

Legal and Regulatory Framework: The General Data Protection Regulation started applying on May 25, 2018, establishing a standardised data protection system in the entire EU member states and even companies that handle the personal data of EU residents, regardless of their location. The GDPR places significant liability on organisations, whether it be the implementation of solid technical and organisational security measures or the requirement to have organisations must designate a Data Protection Officer (DPO) when necessary and perform a DPIA in cases where data-handling activities involve potential risks.

An important point of note is the mandatory breach notification provision, which compels the organisations to report to the supervisory authorities of any data breach to the authorities within 72 hours of knowing about the breach.[21] Non-compliance with GDPR may impose severe fines, amounting to up to 20 million or 4 percent of a company's annual global turnover, whichever is larger, as well as the risk of reputational damage and legal claims by the individuals involved. Due to such heavy fines and the risk of poor publicity, businesses have a strong incentive to purchase cyber insurance benefits.

Cyber Insurance in India: The concept of cyber insurance is quite new to the insurance industry in India. Originally, the policies primarily covered the old-school risks such as fire, property, and health. However, with the explosion of digital tech in the early 2000s and the increase in online banking, e-commerce, and IT services, people became aware of cyber dangers. Previous Indian cyber policies were restrictive and provided very minimal protection and targeted large corporate IT companies rather than SMEs or individuals. The industry estimates the market to be approximately $10 million, back of 2014. The rise in cyberattacks and tougher regulations has since transformed the environment. It has already expanded to approximately

[21] General Data Protection Regulation 2016

500m in 2024, with forecasts estimating approximately over 6.9billion in 2030, with a CAGR of 29.[22]

Legal and Regulatory Framework: The legal and regulatory climate in India is a determining factor when it comes to the development and usage of cyber insurance.

Two key elements influence this trend –

IRDAI Guidelines: The Insurance Regulatory and Development Authority of India (IRDAI), the statutory body overseeing the insurance sector, has encouraged insurers to design and market cyber insurance products as part of its objective to enhance risk protection in the digital economy. The regulator recommends that insurers develop policies that will suit individuals, SMEs, and large corporations so that they are widely accessible. It also requires clarity of policy words to eliminate controversies and encourage transparency.

Effects: These recommendations have resulted in innovation in the market and a rise in confidence of insurers to provide end-to-end cyber-cover.

Digital Personal Data Protection Act, 2023 (DPDP Act): India has a landmark law on data protection, the DPDP Act, 2023.[23] It places heavy responsibilities on the so-called data fiduciaries (organisations that process personal data). Important compliance requirements are reporting data breaches to the Data Protection Board, making sure that personal data is lawfully processed and with the consent of the user. Non-compliance requirements are facing heavy fines of up to 250 crores per violation.

Effects: Organisations are no longer spared as they face high financial risks in terms of data breaches or regulatory violations. This puts a heavy pressure on the need to buy cyber insurance since it can pay the expenses incurred as a result of: regulatory penalties (where legally permissible), legal fees and litigation expenses, incident response and remediation outlays.

[22] Meha Agarwal, 'Insurtech At A Crossroads: What 100% FDI Means For Insurance Startups' (*Inc42*, 06 February 2025) <https://inc42.com/features/insurtech-at-a-crossroads-what-100-fdi-means-for-insurance-startups/> accessed 25 October 2025

[23] Digital Personal Data Protection Act 2023

LEGAL CHALLENGES

Data Protection Laws (GDPR, DPDP Act, HIPAA): The Data protection laws in modern times, such as GDPR in Europe and the DPDP Act of India and HIPAA of the United States, have established a benchmark that a high organisation engaged in the processing of personal data must reach.

Practically, the result of these laws is to present us with a complete round of legal and working headaches, including –

Ambiguous Legal Requirements: GDPR uses terms such as reasonable protection or undue delay, which remain quite vague, and until the court intervenes, we are left guessing.

Compliance Complexity: We are forced to establish structures of express permission, designate a Data Protection Officer, conduct routine audits and maintain records. To smaller companies and startups, that would translate to a hefty price tag, particularly under DPDP.

Cross-Border Issues in Data Transfer: The transfer of personal information across borders is highly restricted and sometimes requires an elaborate government consent that which cripples international businesses.

Risk Management in Health Care: HIPAA compels a yearly risk examination as well as timely corrections of any deficiencies in security, with significant fines in the event of our failure.

These structures are different across regions, yet the similarity here is that we have to remain proactive in terms of data handling, we need to remain transparent to regulators, and we need to continue to adjust to newer directions as they arise.

Attribution of Cyberattacks: One of the major legal and policy dilemmas is assigning blame for cyberattacks to perpetrators, particularly those that are perpetrated by state-sponsored organisations or organised crime.

Key Issues include –

Technical and Evidentiary Complexity: To correctly identify the perpetrators, one must perform high-tech analytics and then conduct a strict legal examination. International legal standards of evidence and attribution are problematic in the establishment of countries.

Political and Institutional Obstacles: Public attribution can be frequently affected by geopolitical interests, whereby there are demands of international bodies to complement and even substitute the existing government-based systems. The absence of worldwide norms slows the procedure and obstructs responsibility in the event of attribution challenges or ambiguity.

Legal Impacts: Attribution is important in criminal indictments, sanctions, and insurance claims, yet the fractured state of evidence standards implies that responses could vary across jurisdictions, as was the case with recent indictments of large-scale hacks in the US.[24]

Thus, global cooperation and enforcement are difficult because consensus on the evidentiary levels and mechanisms of accountability is still evolving.

Standardisation of Insurance Contracts: Even the law of insurance contracts is characterised by disagreement over standard terms- particularly the terms involving the exclusions of risks, the scope of coverage, and consumer protection.

The extent to which the insurers are allowed to exert their control over policyholders has been a challenge to the Supreme Court of India and other jurisdictions –

Consumer Rights versus Risk Exclusions: The courts have indicated that there should be a balance between the right of the insurance companies to insure against certain risks and the concept that contracts should be in line with the policy of the people and equity. The use of standard form contracts cannot put consumers at an unfair disadvantage, yet the companies cannot be pressured to cover every risk.

[24] Amanda G. Hill, 'The Ultimate Challenge: Attribution for Cyber Operations' (*Air Command and Staff College*) <https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/WF_70_HILL_THE_ULTIMATE_CHALLENGE_ATTRIBUTION_FOR_CYBER_OPERATIONS.PDF> accessed 25 October 2025

Absence of Standardisation: There is always controversy with unclear wording and imbalanced bargaining positions, where the policyholders are forced to take the terms as they are without any negotiation. The judicial interpretation is one which has been used to effect just results to the extent that weaker parties may be defended, as well as observing the sanctity of the contract.

Progressive Jurisprudence: More recent cases show an increased judicial attention to exclusion clauses and standardised contracts. But the enforceability of any contract remains subject to the changing case law, the policy of the people and a particular situation of the risk allocation.

The standardisation helps to promote transparency and predictability, but problems exist in the issues of interpretation, consumer equity, and responsiveness to new forms of insurance risks.

CONCLUSION

In the modern digital era, cyber insurance is one of the major ways that companies can mitigate risk. Given the increase in threats such as ransomware and supply-chain attacks, regulatory fines, and more, cyber insurance is more than just a matter of money; it is also a way to enhance the efficiency of risk management.[25] It includes data breaches, business interruption, compliance, and reputation damage areas that define how firms are developing resilience. This significance increases when new regulations are introduced, like GDPR in Europe, the Digital Personal Data Protection Act of 2023 in India, or sector-related regulations in the U.S., like HIPAA, which increase the risk and compliance expenses as well.

Although it appears to be a good idea, cyber insurance remains complex. Key among these obstacles is how to determine who initiated the cyberattack, the fact that there is no universal policy language across nations, the uncertainty over what regulation fines are reimbursed, and the constantly changing threat environment that insurers have to match. But these issues also give openings to novel concepts: smarter models of underwriting, risk checks powered by AI, and cleaner templates of a contract that reduce confusion.

[25] 'Cyber: The changing threat landscape Risk trends, responses and the outlook for insurance' (*Allianz*) <https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/agcs-cyber-risk-trends-2022.pdf> accessed 25 October 2025

Here, the future of cyber insurance will depend on the balance struck: Enhancing business continuity, compliance and resilience with its strengths; As it manages its challenges, including legal grey spaces, systemic risks, and the difficult task of pricing quickly changing cyber threats, it handles them carefully. Finally, cyber insurance is no substitute for sound cybersecurity. It is a complementary armour, a financial and strategic weapon that enables businesses to survive and even thrive in the digital risk epoch.