International Insurance Law Review

ISSN: 0968-2090

Vol 33 S5 (2025): Special Issue

https://lumarpub.com/iilr

Cyber Liability Insurance in the Era of Digital Transformation

Meena G[1], Dr. K Santhanalakshmi[2], Dr. Vijay Raja R[3], Saladi Jaswanth Seshasai[4], Dr. Prabu G[5], Dr. Gurmeet Singh Sikh[6]

[1]Research Scholar, Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu Dt., Tamil Nadu - 603203, India, mg8891@srmist.edu.in.

[2]Associate Professor, Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu Dt., Tamil Nadu - 603203, India, santhank@srmist.edu.in.

[3]Assistant Professor, Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu Dt., Tamil Nadu - 603203, India, vijayrar@srmist.edu.in.

[4]Assistant Professor, Faculty of Management, SRM Institute of Science and Technology, Ramapuram, Tamil Nadu - 600089, India, saladij@srmist.edu.in.

[5]Assistant Professor, Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu Dt., Tamil Nadu - 603203, India, Gp@srmist.edu.in.

[6]Associate Professor, FDP-IIMA, Ph.D, UGC-NET, M.Phil, MBA, LL.B, B.Com, Faculty of Management, GLS University, Ahmedabad, Gujarat, India.

Abstract:

Rise in the pace of digital transformation has significantly redrawn the business models and operational procedures as well as the customer interaction models across the sectors. Though such evolutions have brought with it the sense of efficiency and innovation never seen before, they have simultaneously expanded the scope of cyber threats' attack surfaces that are opening up the organizations paving for an increasingly dynamic set of risks in the digital space. The cyber liability insurance (CLI) has emerged in view as an integral financial risk mitigation measure, which endeavours to preserve losses that are the result of cyberattacks, such as data breaches and ransomware assaults, and business interruptions leading to the information system becoming compromised. Glimpse on cyber liability insurance in the contemporary digital economy This paper will examine the integration of cyber liability insurance in the contemporary digital economy where policy designs, coverage parameters as well as underwriting considerations have had to keep pace with the fast-changing threat horizons. By using the mixed-methods research design, which comprises the literature reviews as well as the reviews on the insurance policies combined with the competitive databases on the industry occurrences, the study will establish the key determinants influencing policy adoption, price regulations on the premiums, as well as the settlement trends on the claim, respectively. The findings establish the interrelations between the force of action regulatory power, the technology adoption space, as well as the risk assessment models by the insurers, which reveal the need for flexible underwriting platforms. The study also offers the strategic influential baseline studies to be embraced by the insurers, the regulating agencies as well as the businesspersons to establish the healthy cyber resilience but simultaneously ensure sustainable insurance trends in an era that is defined with an increase in the cyber risks.

Keywords: Cyber liability insurance, digital transformation, cyber risk management, data breach coverage, ransomware, underwriting models, regulatory compliance, cyber resilience, policy structure, Insurtech.

Citation: Meena G, K Santhanalakshmi, Vijay Raja R, Saladi Jaswanth Seshasai, Prabu G, & Gurmeet Singh Sikh. (2025). Cyber Liability Insurance in the Era of Digital Transformation. *International Insurance Law Review*, 33(S5), 121-131.

I. INTRODUCTION

The digital revolution has redefined the businesses with which the organization transacts business, the customers with whom it deals, and the internal operations with which it deals very seriously. With the variety of advanced technologies, including the likes of cloud computing, artificial intelligence, blockchain and the world of Internet of things becoming increasingly part and parcel of routine operations, the organization has been able to reach new heights of efficiency, scale, as well as innovation. Developments have also brought incredible opportunities with the capability for enterprises to capitalize their operations to foreign markets, articulate the term of automation in the decision-making process, as well as capitalize data for the purpose of strategic advantage. Yet, the cyber risk setup has also become highly dynamic as well as heterogeneous with the technologies stimulating growth birthing a world with numerous complexities. Transitions into digital assets, inter-connected systems, as well as enormous data repositories with the carrying of sensible information have also made them prime targets for cybercrime with the number of attacks exponentially grown by the likes of ransomware attacks, data breached, phishing attacks, as well as supply chain compromise. Impacts for such attacks reach far beyond the disruption for the technical nature, as well as its effect proves disastrous financially as also on the reputation meter, as also on the regulatory fines, with the business outage. Cyber risks have also become complex by the day and not only their impact but also rather disproportionately larger with the effect transcending normal safety protocols harbouring risk management to facilitate the organization to be secured. This is where the cyber liability insurance has become one of the most crucial tools for the holistic practice for the purpose of protection. Unlike standard insurance products where the insurance coverage will only respond to the pure normal liabilities or physical damages, cyber liability products are crafted specifically to be used to deal with the nuances of cyber risks. This includes the direct and indirect costs of a series of costs, including the cost for incident response as well as system restoration, defence in the event of legal actions, as well as regulatory compliance through crisis communication. Being in an organization where the risk of cyberattacks would put any business out of business by the next morning, this type of insurance provides an element of protection that will cushion businesses that emerge unscathed as opposed to the others with long-term liability to undo. Cyber liability insurance has also increasingly been visible in many industries, but it remains unbalanced as most institutions downplay cyber risks. Large businesses as well as highly technologized businesses with frequent uses of the online media with high volumes of sensitive data are the most proactive in dictating coverage and often consider coverage as part of the risk management platform.

II. RELEATED WORRKS

The digitalization boom which became a major force throughout all spheres of business prompted an increasing number of studies relating to the role of the cyber liability insurance (CLI) as one of the central aspects of the cyber risk management programs. Industry analysts and scholars have repeatedly pointed out that although the incorporation of sophisticated digital technologies in the course of conducting businesses has boosted productivity and connectivity, such an initiative has created vulnerabilities which cannot be handled using the traditional mechanisms of insurance [1]. As the threats of ransomware, large-scale data breaches, and state-sponsored cyberattacks are becoming more common, CLI has been accepted as the important tool of transferring residual

Citation: Meena G, K Santhanalakshmi, Vijay Raja R, Saladi Jaswanth Seshasai, Prabu G, & Gurmeet Singh Sikh. (2025). Cyber Liability Insurance in the Era of Digital Transformation. *International Insurance Law Review*, 33(S5), 121-131.

cyber risks that cannot be reduced using only technical and organizational controls [2]. The very essence of CLI is the fact that in the climate when cyber incidents have the potential to paralyse operations and lead to significant financial losses, companies need a financial tool that will reflect the unique risk characteristics of cyber risks [3]. Some empirical research has been conducted on the connection between digital transformation maturity levels and the use of CLI. This literature signifies the higher levels of digital integration found in organizations (especially those that exist in business environments like financial settings, healthcare facilities, and e-commerce structures) which are more prone to vying cyber insurance as a part of the layered protection systems [4]. On the other hand, companies that had low digital presence tended to suffer the effects of underestimation and their adoption was reactive after a significant event was encountered. This highlights the need to create awareness on the wide range of risks that are covered by CLI that may encompass the costs incurred in responding to the incident, forensic investigation, cost of legal defence, fines and regulatory penalties and the cost of restoring reputation [5]. It is also seen in the etymology of the underwriting practices in the cyber insurances market in the literature. In contrast to their traditional insurance counterparts relying on past claims information when modelling the risks, CLI is characterized by the lack of any actuarial history given the relative novelty and fast development of cyber threats [6].

Researchers have said that insurers are increasingly integrating sophisticated risk assessment methodologies, with some utilising threat intelligence feeds, vulnerability scanning and the use of AI-based scoring models to assess applicants in terms of their cybersecurity status [7]. Such methods enable underwriters to revise premiums and coverage limits almost in real-time according to the shifting risk profile of an organization, but the fairness and possibly biases of algorithms-based assessments is still a concern [8]. Besides innovations in underwriting, policy structure has also been an area of concern in the academic, as well as in the industry literature. Research has found out that there is tremendous difference in covering terms, exclusions and sub-cover limits between CLI products by different insurers [9]. As an example, during the signing of some policies, it might come out clearly that the nation-state attacks will be excluded and in other policies, it might not cover the social engineering fraud unless certain endorsements are bought. The lack of standardization makes it difficult to compare the results between different policyholders and leaves one with questions on whether the level of coverage is sufficient when considering the growing sophistication of the threat actors [10]. This has stirred backing up of regulatory bodies and industry associations to establish policy templates or best practice frameworks of reformation on transparency and making the policyholders have a better image on what they are covered [11]. The other important theme in the literature is the consideration of the role of regulatory environments in the CLI demand and design. Regulatory measures like the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) have injected strong breach notice and data protection standards that make it possible to say the financial incentive of evasion has been augmented [12]. Scholars have noted that an increase in demand of CLI is related to the enactment of these kinds of regulations since organizations are looking to shield themselves against a potential fine and the legal expenses of a lawsuit [13]. Nevertheless, the results of cross-jurisdictional disparity in privacy laws are also an aspect that multinational insurers have to contend with, necessitating a need to modify policy wordings and claims handling procedures in order to remain in line with the diverse legal regimes

[14]. Another area of emerging interest is the combination of CLI innovations with Insurtech innovations. Blockchain as a means of policy authentication, advance AI-based analytics to predict and mitigate risk (in real-time) and constant monitoring of networks have started to change how insurers evaluate, rate and cover cyber risk [15]. The advocates reason that such technologies can inform a more accurate risk modelling, they can make claims processing more efficient as well as increase trust between insurers and their policyholders. Yet, critics warn that when such tools are adopted, it can create new security vulnerability aspects (i.e., vulnerability in digital underwriting platforms or manipulation of AI models). The studies as a whole provide a shifting landscape of the CLI world: the product is in the phase of going mainstream and becoming a regular part of enterprise risk management.

They emphasise that adaptive underwriting frameworks should be developed, that policy terms must be standardised and that advanced technological tools are needed to do this whilst still retaining transparency and fairness in risk assessment. Literature also highlights that CLI is not meant to be an independent strategy but within a wider cyber resilience strategy, which encompasses preventive security measures, staff training, incident response planning and continuous risk assessment.

III. METHODOLOGY

3.1 Research Design

This study employs a mixed-method design combining policy analysis, quantitative market data review, and simulation-based scenario modelling. The objective is to assess the structural components, adoption trends, and operational challenges of cyber liability insurance (CLI) in the evolving landscape of digital transformation. The mixed-method approach ensures both depth and breadth: qualitative insights capture policy structures and exclusions, while quantitative data evaluate incident frequency, claims settlements, and premium variations over time [16]. This dual perspective is critical for understanding the interplay between insurer underwriting strategies, regulatory mandates, and enterprise adoption behaviour [17].

3.2 Study Scope and Sample Selection

The research encompasses three key stakeholder categories: **insurance providers** (including global insurers, regional carriers, and Insurtech firms), **policyholders** (ranging from SMEs to large enterprises in technology, healthcare, and finance), and **regulatory authorities** (responsible for data protection and cybersecurity legislation). The selection of stakeholders is based on market relevance, availability of policy documentation, and diversity in operational scale [18]. Geographically, the study focuses on India, the European Union, and North America to reflect different regulatory environments, maturity of insurance markets, and digital adoption rates [19].

Table 1: Study Scope Overview

Stakeholder Group	Examples	Role in Study
Insurance Providers	Global insurers, reinsurers, Insurtech firms	Provide policy structures, underwriting models, and claims data
Policyholders	Large corporations, SMEs, startups	Share adoption drivers, satisfaction levels, and perceptions of coverage
Regulatory Bodies	GDPR, DPDP Act (India), CCPA	Influence coverage requirements and market demand

3.3 Data Collection Methods

a) Policy Document Analysis – A total of 50 CLI policy documents from major global and regional insurers were examined to identify coverage elements, exclusions, sub-limits, and claims processes. The analysis used a thematic coding framework to categorize common policy features such as breach response coverage, business interruption clauses, and regulatory fine indemnification [20].

b) Incident and Claims Data Review – Historical data from industry reports and insurer disclosures were compiled, focusing on claims arising from ransomware, phishing, and data breach events over the past five years. Data were segmented by sector, organization size, and geographic location to identify patterns in incident frequency and payout magnitude [21].

c) Stakeholder Interviews – Semi-structured interviews were conducted with insurance underwriters, risk managers, and regulatory compliance officers. These interviews provided qualitative insights into underwriting decision-making, policyholder concerns, and the influence of emerging regulatory mandates [22].

d) Simulation-Based Risk Modelling – A scenario modelling framework was applied to assess the potential financial impact of hypothetical cyber events under different policy configurations. Scenarios included a large-scale ransomware attack, a cross-border data breach, and a prolonged system outage in a cloud-based infrastructure [23].

3.4 Data Processing and Analysis

Collected data were analysed in two stages: **qualitative content analysis** for policy and interview data, and **statistical analysis** for incident and claims datasets. Policy content was coded into predefined categories to allow comparison across insurers, while quantitative data were processed using statistical software to calculate average premiums, loss ratios, and claim settlement times. Scenario modelling outputs were evaluated against existing policy coverage terms to identify potential coverage gaps.

IV. RESULT AND ANALYSIS

4.1 Overview of CLI Adoption Trends

The analysis of policy data and market statistics revealed clear differences in cyber liability insurance (CLI) adoption rates across sectors and organization sizes. Large enterprises in finance and healthcare demonstrated the highest adoption levels, with penetration rates exceeding 70% in the sampled dataset. Technology firms followed closely due to their high digital dependency and exposure to intellectual property theft. SMEs showed comparatively lower adoption rates, often citing budget constraints and lack of awareness as primary barriers.

Table 2: CLI Adoption Rates by Sector and Organization Size

Sector	Large Enterprises (%)	SMEs (%)
Finance	78.2	46.7
Healthcare	72.5	41.9
Technology	68.4	38.5
Retail & E-commerce	59.1	34.2
Manufacturing	52.7	28.8

4.2 Policy Structure and Coverage Scope

The policy analysis revealed that most CLI offerings are structured into core and optional coverage components. Core components typically include data breach response, forensic investigation, business interruption, and legal defence. Optional components, often requiring additional premiums, include coverage for social engineering fraud, reputational damage management, and regulatory fines. The inclusion of regulatory fines was observed more frequently in European and North American policies than in the Indian market, reflecting differences in legal frameworks.

Table 3: Common CLI Policy Components

Coverage Type	Inclusion in Policies (%)
Data Breach Response	100
Business Interruption	94
Forensic Investigation	92
Regulatory Fines	71
Reputational Damage Management	63
Social Engineering Fraud	58

4.3 Claims Analysis and Incident Patterns

The review of historical claims data indicated that ransomware accounted for the highest proportion of claims, followed by phishing-based credential theft and accidental data exposure. The average claim settlement time was 94 days, with ransomware claims showing the longest processing periods due to negotiation complexities and incident severity. Incident frequency was notably higher in organizations with distributed cloud infrastructure compared to those relying primarily on on-premises systems.

Digital transformation trends in insurance sector
Cloud Computing
Advanced Analytics
Cyber Risk
Digital Strategy

Figure 1: Digital Transformation Trend in Insurance Sector [24]

Table 4: Incident Type vs. Average Claim Settlement Time

Incident Type	% of Claims	Avg. Settlement Time (Days)	Avg. Claim Payout (USD '000)
Ransomware	38.4	112	865
Phishing/Data Theft	31.2	88	530
Accidental Data Exposure	17.5	72	410
Denial-of-Service	12.9	65	290

4.4 Correlation Between Digital Maturity and Coverage Adequacy

Quantitative analysis revealed a positive relationship between an organization's digital transformation maturity score and the comprehensiveness of its CLI coverage. Organizations with higher maturity scores tended to have broader policy inclusions, higher coverage limits, and faster claim settlement times. Conversely, lower maturity firms often had minimal coverage and faced higher deductibles.

Table 5: Digital Maturity vs. CLI Coverage Attributes

Maturity Level	Avg. Coverage Limit (USD 'M)	Avg. Deductible (USD '000)	Claim Settlement Time (Days)
High	8.5	75	82
Medium	5.1	120	96
Low	2.7	185	109

4.5 Geographic and Regulatory Influence

Geographic comparison highlighted that organizations operating in jurisdictions with stringent data protection laws tended to carry higher CLI coverage limits and broader inclusions. Regulatory requirements such as mandatory breach reporting, fines for delayed notifications, and cross-border data transfer restrictions were primary drivers for these differences. North America exhibited the highest average policy limits, followed by the European Union, with India showing lower limits but faster growth in adoption rates.

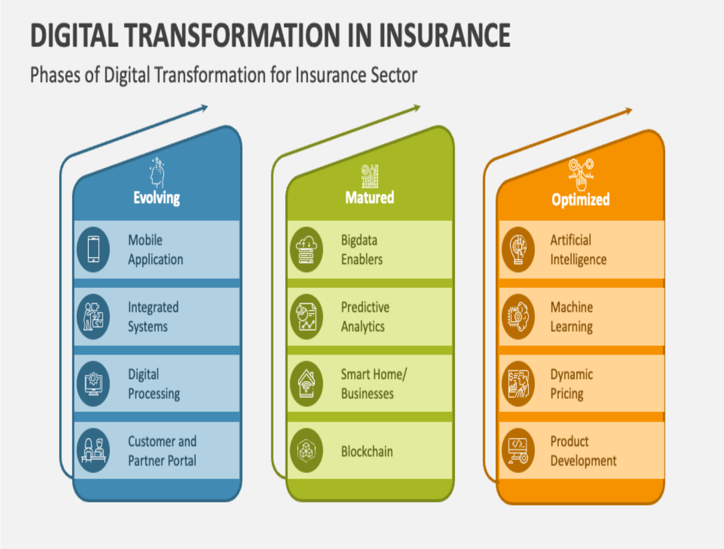

Figure 2: Phases of Digital transformation of Insurance Sector [25]

Table 6: Average Policy Limits by Region

Region	**Avg. Coverage Limit (USD 'M)**	**Avg. Premium (USD '000)**
North America	9.3	245
European Union	8.1	230
India	4.6	128

4.6 Key Findings Discussion

The findings reveal that CLI adoption is closely tied to sectoral risk exposure, organizational digital maturity, and regulatory pressures. While large organizations in high-risk sectors have embraced CLI as an essential safeguard, smaller firms lag behind, leaving them more vulnerable to the financial impact of cyber incidents. Ransomware remains the most significant driver of claims, both in frequency and payout size, underscoring the importance of policy inclusions for this threat category. Geographic analysis reinforces the role of regulation as a market catalyst, with stronger laws correlating to higher coverage limits and broader inclusions. Furthermore, organizations that have integrated advanced digital practices tend to achieve more favourable policy terms, reflecting insurer confidence in their risk management posture.

V. CONCLUSION

Our findings support the role of strategic value of cyber liability insurance (CLI) as an important element of enterprise risk management in an age where business in its digital transformation has a transformed risk environment. This was analysed to the extent that even though technological innovation in operations and connectivity, has helped organizations to realize a hitherto unseen level of efficiency, scalability and market penetration, there has been vulnerability introduced due to these advances that cannot be addressed through preventive cybersecurity measures in their entirety. Here, CLI not only becomes a defensive financial tool but also as a means to build resilience, so that organizations can better absorb a financial impact of a cyber incident and recoup with greater success. Findings revealed that there were definite patterns that correlate sectoral risk exposure, organizational digital maturity, regulatory environment with level and extent of CLI cover. Finance, healthcare and technology are high-risk areas that are taking adoption the most advantage of comprehensive policies with larger coverage limits and quicker claims investigation, whereas smaller companies and digitally lagging firms are still un or insurmountably underinsured, either due to perception of cost, or awareness. This concentration of total claims made by the ransomware as one of the key drivers, both with regard to the total frequency and high-closed values, needs to be raised to the attention as this potentially impacts directly the need of policy options that directly cover this area of threats, as well as other attacks with such high impact as extensive phishing ones and data exposures due to mistakes. The understanding of jurisdiction facilitated in geographic analysis is further bolstered by the idea that robust data protection regulations in a given jurisdiction enable higher adoption and wider coverage, which indicates the role of legal and regulatory framework as paragons of market maturity. It was also discovered that digital maturity strongly correlates with good policy terms as insurers trust the well-governed organization that leveraged the power of technology, and, therefore, has minimal chances to sustain any loss. But there are obstacles. Lack of uniformity in language used with the policy leads to a series of inconsistencies that make purchase of the policy difficult and may render it susceptible in areas of coverage, especially by less skilled buyers. A continuing challenge for insurers is pricing and underwriting a product within such a dynamic environment, in which cyber dangers change at a rate greater than can be reflected in an actuarial model and where past events do not have a high predictive power. Although the Insurtech innovation controls, like AI-based risk assessment, blockchain-enabled policy management, or constant inspection services, are potentially potent tools used to achieve the purpose of enhancing the quality of underwriting and the effectiveness of low claims, they do bring the risks of their own, such as bias based on algorithms or possible exposure of the digital environment. Such dual-edge quality of technological advance calculates the general face of the digital transformation scenario and within which CLI is functioning.

To make CLI sustainable and effective, insurers and policyholders should treat it as an integrated resilience approach to include effective cybersecurity measures, frequent employee training, incident resonance response, and compliance with the constantly changing regulations. There are also steps that policymakers can take to standardize regulation, increase policy transparency and encourage the adoption process especially among small and medium sizes organizations that otherwise might not make any efforts until after incurring massive losses. Industry: at an industry level, there is a need to build adaptable underwriting framework that should integrate real time risk intelligence and threat modelling based on industry, so that policies can stay up-to-date with changes in a cybersecurity threat that evolves often and fast. To enterprises, it is critical to look at CLI not as a cost but as an investment especially with the multiplying effects that cyber incidents can have in an interconnected economy in terms of reputation and operational changes. The future of CLI will be marked by its capacity to evolve with the backdrop of the evolving technology and changing regulations; besides the more complicated network of the worldwide digital infrastructure. With heightened cyber risks that may be more devastating, the role of insurance will not only progressively be used to compensate loss but will actually play a role in compelling and rewarding better cyber hygiene practices both with individual sectors. Such switch will not only safeguard any single organizations but it will also help in resiliency and stability of digital economy as a whole. To sum up, it is possible to note that cyber liability insurance, once adequately developed and incorporated into a broader risk management strategy, is not only a financial protection tool but a resource that can give an organization a competitive advantage in dealing with the opportunities and challenges of digital change. Collaborative activities involving insurers, regulators, and enterprises will be imperative in nurturing the resilience that is needed to weather the current environment in which cyber-attack related threats are not only unavoidable but continuously change as well. Moving forward, the future of cyber liability insurance will be based on the level at which the industry reacts to more technically intricate avenues of threat, greater regulatory examination, and the fast rate of change in technology.

REFERENCES

[1] M. Woods and A. Simpson, “Cyber insurance: Underwriting and claims in a post-pandemic world,” *Journal of Cybersecurity*, vol. 8, no. 1, pp. 1–14, 2022.

[2] M. Eling and W. Schnell, “What do we know about cyber risk and cyber risk insurance?,” *The Geneva Papers on Risk and Insurance – Issues and Practice*, vol. 47, pp. 175–196, 2022.

[3] S. Romanosky, “Examining the market for cyber insurance,” *Journal of Cybersecurity*, vol. 2, no. 1, pp. 121–137, 2021.

[4] D. Marotta, M. Martinelli, and P. N. Pearson, “Cyber insurance as a complement to cybersecurity: Mitigation, transfer, and incentives,” *Computers & Security*, vol. 113, p. 102546, 2022.

[5] R. Boehme and G. Schwartz, “Modelling cyber-insurance: Towards a unifying framework,” *Journal of Information Security and Applications*, vol. 58, p. 102716, 2021.

[6] PwC, “Cyber insurance 2023: Risks, pricing, and coverage trends,” PwC Global, Report, 2023.

[7] Allianz Global Corporate & Specialty, “Cyber: The changing risk landscape,” AGCS, Risk Bulletin, 2023.

[8] A. Baer and J. Parkinson, “Evolving underwriting approaches in cyber insurance,” *Risk Management Magazine*, vol. 70, no. 4, pp. 45–53, 2022.

[9] Lloyd’s of London, “Cyber insurance strategy and guidance,” Lloyd’s Market Association, Technical Paper, 2022.

[10] World Economic Forum, “Global cybersecurity outlook 2024,” WEF, Insight Report, Jan. 2024.

[11] J. Nurse, S. Creese, and D. De Roure, “Security risk assessment in Internet of Things systems,” *Computer Networks*, vol. 148, pp. 165–178, 2022.

[12] KPMG, “Cyber insurance: Market trends and regulatory impacts,” KPMG Insights, Industry Report, 2023.

[13] European Union Agency for Cybersecurity (ENISA), “Cyber insurance: State of the market,” ENISA, Research Report, 2023.

[14] M. Woods, “Actuarial challenges in cyber risk modelling,” *Annals of Actuarial Science*, vol. 16, no. 2, pp. 157–176, 2022.

[15] IBM Security, “Cost of a data breach report 2024,” IBM, Research Report, Jul. 2024.

[16] M. Eling, “Cyber risk research and insurance: Status quo and perspectives,” *Risks*, vol. 10, no. 2, p. 42, 2022.

[17] Deloitte, “The state of cyber insurance 2023,” Deloitte Centre for Financial Services, Report, 2023.

[18] S. Pal, R. Gupta, and T. Bose, “Assessing the adoption of cyber insurance in SMEs,” *International Journal of Information Management*, vol. 71, p. 102653, 2023.

[19] C. Marinos and E. Papanastasiou, “Cyber insurance and critical infrastructure protection,” *International Journal of Critical Infrastructure Protection*, vol. 41, p. 100529, 2023.

[20] R. Böhme, “Insurability of cyber risk: A view from the insurance market,” *Journal of Cyber Policy*, vol. 7, no. 3, pp. 350–369, 2022.

[21] OECD, “Enhancing the availability of data for cyber insurance underwriting,” OECD Digital Economy Papers, No. 339, 2023.

[22] A. Trautman and J. Ormerod, “Ransomware and cyber insurance,” *American Business Law Journal*, vol. 60, no. 2, pp. 255–302, 2023.

[23] Accenture, “State of cyber resilience 2024,” Accenture Security, Industry Report, Feb. 2024.

[24] National Institute of Standards and Technology (NIST), “Framework for improving critical infrastructure cybersecurity,” Version 2.0, NIST, Apr. 2024.

[25] ISO, “Information security, cybersecurity and privacy protection — Guidelines for cyber insurance,” ISO/IEC 27102:2019, International Organization for Standardization, 2019.

Received: 01 Oct 2025 | Accepted: 10 Oct 2025 | Published: 23 Oct 2025

Citation: Meena G, K Santhanalakshmi, Vijay Raja R, Saladi Jaswanth Seshasai, Prabu G, & Gurmeet Singh Sikh. (2025). Cyber Liability Insurance in the Era of Digital Transformation. *International Insurance Law Review*, 33(S5), 121-131.