PANJAB UNIVERSITY LAW REVIEW
ISSN: 0971-5541, Volume 64, Part 2, pp. 95-107

NAVIGATING INSURANCE FRAUD IN CYBERSPACE: LEGAL AND REGULATORY ISSUES IN INDIA

Dr. Zubair Ahmed Khan[*]
Dr. Vikeash Ram Tripathi[**]

ABSTRACT

Insurance fraud is not a new phenomenon in the insurance business, but the diversity of fraudulent practice it now encompasses produces adverse effects across every dimension of the sector. In the digital age, insurers rely heavily on internet-based operation to conduct business efficiently and to manage insurance risk, yet this dependence on technology exposes the sector to a distinct category of cyber risk, including data breach and cyberattack, capable of inflicting substantial financial loss on both insurer and insured. This paper examines the legal and regulatory framework governing insurance fraud in cyberspace in India, analysing the statutory foundations of insurance contract law, the evolving typology of cyber-enabled insurance fraud, and the regulatory response the Insurance Regulatory and Development Authority of India has developed through successive cybersecurity and fraud-monitoring guidelines. It argues that while India's regulatory architecture has matured considerably, from the 2017 cybersecurity guidelines through the 2023 Information and Cyber Security Guidelines to the 2025 Insurance Fraud Monitoring Framework Guidelines, this architecture remains only loosely integrated with the broader statutory framework the Digital Personal Data Protection Act, 2023 supplies, and the paper proposes closer alignment between insurance-specific regulation and general data protection law as the principal reform India's cyber-insurance governance requires.

KEYWORDS: *Insurance Contract; Insurance Fraud; Cybersecurity; Cyber Insurance; IRDAI*

1. INTRODUCTION

The Indian insurance industry has witnessed significant growth in step with the country's economic expansion. Around fifty crore people now have access to health insurance under the Central Government's Ayushman Bharat-Pradhan Mantri Jan Arogya Yojana scheme, and more than sixty-five per cent of the country's population is presently covered by some combination of government-supported and commercial health insurance.[1] Insurance, in its ordinary legal sense, is a contract under which the insured obtains financial protection in the form of reimbursement against a defined category of loss, the insurer pooling client risk to render the resulting payment obligation more affordable; life insurance provides for payment upon death, terminal illness or the expiry of a policy term depending on its specific conditions, while general or non-life insurance provides payment upon the occurrence of a defined financial event other than death. As the Indian insurance sector has grown in scale and product complexity, it has confronted mounting operational challenge, including

[*] Associate Professor, University School of Law & Legal Studies, Guru Gobind Singh Indraprastha University, New Delhi.
[**] Assistant Professor, Faculty of Law, University of Delhi.
[1] IRDAI-NHA Joint Working Group, Report of Sub-group on Fraud Control (Insurance Regulatory and Development Authority of India, 2019).

pricing, product innovation, policy lapsation and, of central concern to this paper, fraud management.

The COVID-19 pandemic accelerated this challenge considerably by shifting substantial business operation toward remote working models, complicating enforcement of conventional security measures including endpoint encryption and controlled network access. Digital technology's benefits in efficiency and productivity accordingly arrive bundled with the "digital security risk" of compromised confidentiality, integrity and availability of information and information systems, a risk statistics confirm is intensifying: one-third of the countries the World Economic Forum surveyed across the Organisation for Economic Co-operation and Development in 2017 ranked cyber risk among their top two business risks, ahead of both terrorist attack and natural disaster, and fifty-three per cent of cyberattacks surveyed in a separate industry report resulted in losses exceeding fifty thousand dollars.[2] India's own exposure is acute: by the third quarter of 2021 India was the fourth most heavily ransomware-affected jurisdiction in Asia, the average cost of an Indian data breach stood at $2.21 million, and more than eight billion records were compromised globally in the first quarter of 2020 alone, developments that have driven rapid growth in cyber insurance uptake and are projected to push the global cyber insurance market to twenty billion dollars by 2025.[3] Because the insurance sector manages an unusually large volume of sensitive personal, medical and financial data, it constitutes a particularly attractive target for cyber-criminal activity, and sophisticated spoofing fraud has already compromised corporations at the highest levels of the healthcare, aviation and hospitality industries.

1.1 Objective of the Study

This study examines how the nature of the insurance contract operates within cyberspace, assessing the distinctive character of cyber-enabled insurance fraud as a sophisticated category of financial crime and evaluating the degree of insurance risk such fraud generates for insurers, insured parties and the broader financial system, with a view to identifying the regulatory reform India's insurance sector requires to address it effectively.

1.2 Research Methodology

The methodology adopted is doctrinal, incorporating an analytical review of relevant statute, regulatory guideline and contemporary case law to examine the legal position governing insurance fraud in cyberspace under Indian law.

---

2 World Economic Forum, The Global Risks Report 2017 (12th ed. 2017); IBM Security, Cost of a Data Breach Report 2021 (2021).

3 Risk Based Security, Q1 2020 Data Breach QuickView Report (2020); Munich Re, Cyber Insurance: Risks and Trends (Apr. 2020).

2. INSURANCE FRAUD: CONCEPT AND STATUTORY FOUNDATIONS

Financial fraud poses a serious risk to every component of the financial sector, and any fraudulent conduct within the insurance industry directly reduces consumer confidence and damages institutional goodwill. Insurance fraud may be understood as a strategic, pre-concerted mechanism through which a party, by wilful deceptive practice or concealment of fact, obtains an unfair advantage while causing pecuniary loss to an aggrieved party, including the insured; such conduct may proceed through unauthorised access to private information, misused by an insurance agent, an employee of the insurer, or an anonymous third party who has breached cybersecurity protection, and it typically manifests in the multiplication of premium demanded of subsequent policyholders as insurers price the resulting risk into their broader book of business.[4] The Insurance Regulatory and Development Authority, recognising this responsibility, introduced the IRDA (Preparation of Financial Statements and Auditors' Report of Insurance Companies) Regulations, 2002, obliging the management of every insurance entity to streamline internal processes to secure resources against manipulation and fraudulent activity on an annual basis, and has since developed fraud-assessment guidelines requiring insurers to detect, mitigate and periodically report fraud data in a prescribed format.

Fraudulent conduct in the insurance sector spans several distinct categories. Policyholder fraud typically arises at the point of sale or claim, through fabricated or inadequate documentation supporting fictitious or exaggerated loss, a pattern especially prevalent in health and medi-claim insurance where forged medical receipts and treatment records are submitted to support a claim; such conduct may include outright fabrication of a claimed event, deliberate exaggeration of otherwise genuine loss, or submission of records that misrepresent the nature or extent of medical treatment actually received. Distribution fraud arises where agents or intermediaries misrepresent risk to secure reduced premium, inflate the premium quoted to a policyholder while reporting a lower figure to the insurer, or levy commission inconsistent with the governing insurance agreement; such intermediary-level fraud is particularly corrosive to consumer trust because it occurs at the very point of sale where the policyholder's confidence in the product is first established, and its detection accordingly requires the same institutional vigilance IRDAI's guidelines, examined in Part 5, direct toward distribution channels specifically. Internal fraud arises where directors, managers or staff engage in misappropriation, including manipulated financial records, forged cheques, inflated expenditure, creation of fictitious invoices, undisclosed conflict of interest, and disposal of insurer assets below market value, conduct that exploits the fiduciary position

[4] Monalisha Mohanty, An Insight into Insurance Fraud and Its Prevention, 8(1) J. Ins. Inst. India 19 (2020).

such personnel occupy within the insurance entity and that consequently demands internal control mechanisms distinct from those directed at external or policyholder-originated fraud.

Section 45 of the Insurance Act, 1938 permits a contract of insurance to be called into question within three years of the commencement of risk on grounds of fraud or misrepresentation, and the leading decisions in Mithoolal Nayak v. Life Insurance Corporation of India and P.J. Chacko v. Chairman, Life Insurance Corporation of India confirm that the principle of good faith is foundational to a valid insurance contract, requiring policyholders to disclose material fact in the proposal form without ambiguity or suppression, on pain of forfeiting the policy's benefit where a breach of that good faith is subsequently established.[5] These decisions remain doctrinally significant well beyond their original factual context because they establish the interpretive baseline against which all subsequent insurance fraud, including the cyber-enabled variants this paper examines, continues to be assessed: whatever the technological mechanism through which a given fraud is perpetrated, ransomware-enabled data theft, phishing-induced misrepresentation, or AI-generated fabricated documentation, Indian insurance law continues to test the resulting dispute against the same underlying requirement of uberrima fides, utmost good faith, that Mithoolal Nayak and Chacko articulated in a pre-digital context.

The cyber dimension of insurance fraud has grown alongside the sector's own digital transformation, a trend evidenced in Indian jurisprudence by decisions including Syed Asifuddin v. State of Andhra Pradesh, which confirmed that a telephone handset may constitute a "computer" for the purposes of Section 2(1)(i) of the Information Technology Act, 2000, a provision defining a computer broadly as any electronic, magnetic, optical or other high-speed data processing device performing logical, arithmetic or memory function.[6] This broad statutory definition has proved significant for extending cybercrime provisions to the diverse range of devices through which contemporary insurance fraud is increasingly perpetrated.

3. THE TYPOLOGY OF CYBER RISK TO INSURANCE BUSINESS

Contemporary cyber threats to the insurance sector fall into several recurring categories. Ransomware attack has produced substantial change in policy terms, premium structure and policyholder-data surveillance, its unpredictability compounding the difficulty of detection, since such attacks frequently go unnoticed for weeks or months, deteriorating the trust-based relationship

---

5 Mithoolal Nayak v. Life Insurance Corp. of India, A.I.R. 1962 S.C. 814 (India); P.J. Chacko v. Chairman, Life Insurance Corp. of India, A.I.R. 2008 S.C. 425 (India).

6 Syed Asifuddin v. State of Andhra Pradesh, 2005 Cri. L.J. 4314 (India); The Information Technology Act, No. 21 of 2000, § 2(1)(i) (India).

between insurer and customer. Addressing this threat requires more than a single technical fix; effective response demands regular review of cybersecurity mechanism, integrated security audit, sustained capacity-building against attack, and a coordinated incident-response strategy rather than isolated remedial action following an individual breach. Data breach and theft of sensitive information exploit the large volume of personal, financial and medical data insurers routinely collect, exposing that data to sale on illicit markets through phishing, credential theft or inadequate authorisation protocol, and such breach frequently exposes the regulatory gap between insurance-specific cybersecurity obligation and the broader statutory data-protection framework this paper's analysis in Part 6 addresses directly. Third-party vulnerability arises through the insurance sector's growing reliance on cloud infrastructure, information-technology contractors and claims-management software, each supplying an additional point of potential compromise capable of eroding the integrity of the insurer's own cybersecurity ecosystem regardless of how robust that insurer's internal controls may independently be.

Social engineering attack manipulates policyholders or employees into disclosing sensitive personal or financial data through impersonation, with damage that may begin modestly but escalate into irreversible loss over time; Section 10 of the Digital Personal Data Protection Act, 2023 accordingly supports the case for insurers appointing a data protection officer analogous to that provision's statutory data auditor, while Section 33's penalty regime, calibrated to the frequency and severity of breach and the commercial gain achieved through it, supplies meaningful deterrence against unauthorised access resulting in data compromise.[7] Insider threat presents a distinct challenge precisely because it originates from within the institution's own trusted personnel: an employee with legitimate access to sensitive data may provide unauthorised access to a third party, generating both direct data breach and broader disruption to routine business operation, a risk requiring careful crisis-management protocol and sustained attention to identity-protection practice specifically. Cyber theft encompassing identity and password theft, distributed denial-of-service attack disrupting network accessibility and damaging institutional reputation in a competitive market, and increasingly, artificial-intelligence-enabled attack capable of executing more sophisticated phishing and network intrusion than conventional incident-response protocols are designed to address, complete the principal categories of cyber risk presently confronting the sector; cyber policies accordingly require explicit provision addressing AI-enabled attack, AI-based structural audit and real-time detection capability against AI-driven fraud and deepfake-enabled deception specifically, since typical cyber coverage presently developed for earlier generations of

[7] The Digital Personal Data Protection Act, No. 22 of 2023, §§ 10, 33 (India).

threat does not automatically extend to this newer and rapidly evolving category of risk.

Beyond these specific categories, the insurance sector confronts the general reality that cyber-attack, by compromising system integrity, may generate substantial third-party liability and invite regulatory intervention independent of any direct financial loss the insurer itself sustains. According to the Allianz Risk Barometer 2020, cyber incident now ranks as the most significant threat businesses worldwide face, surpassing supply-chain disruption, legislative change and natural disaster, a ranking the shift toward remote working has reinforced by expanding the practical attack surface available to cyber-criminals exploiting the reduced security oversight remote access typically entails.

4. CYBER INSURANCE: FUNCTION AND MARKET DEVELOPMENT

Cyber insurance offers a mechanism through which corporations and individuals transfer a portion of their financial exposure to insurance markets, though it functions as a complement to, rather than a substitute for, direct investment in cybersecurity infrastructure. A cyber insurance policy typically covers business downtime cost, forensic investigation expenditure, cyber extortion cost, data breach liability and associated legal expenditure, though pricing such coverage has proved genuinely difficult given the constantly evolving character of cyber risk and the corresponding absence of the extensive historical loss data on which actuarial practice conventionally depends. This absence of reliable historical loss data distinguishes cyber insurance from most established lines of insurance business, life, motor or property insurance, each of which benefits from decades of accumulated actuarial experience permitting relatively confident risk pricing; cyber risk, by contrast, evolves so rapidly that loss experience from even three or four years earlier may bear only limited relevance to the threat environment an insurer must price coverage against today, a structural difficulty that helps explain the comparatively conservative and narrowly defined coverage many current cyber insurance products still offer.

Industry leaders accordingly favour a quantitative risk-assessment approach combined with continuous monitoring of the risk environment, seeking objective insight into prospective cyber-risk profile, cost-effective mitigation strategy, and insurance structures tailored to anticipated threat. In India specifically, growing digital-payment adoption has produced a corresponding surge in digital fraud, particularly following the COVID-19 pandemic, prompting insurers to develop dedicated cyber insurance products covering losses arising from malware and phishing attack alongside the legal defence costs such incidents typically generate. This growth trajectory reflects a broader structural shift: as remote working arrangements normalise, individual cyber insurance policies, rather than coverage confined to corporate entities, are

increasingly anticipated to enter the Indian market, extending protection against common cyber threat, including virus attack, phishing, spoofing and loss of personal information, to individual policyholders directly. The market's continued expansion notwithstanding, meaningful gaps in product availability persist, particularly for the emerging categories of loss, SIM-jacking, card cloning and skimming, that Part 5 examines in the context of IRDAI's own product-structure guidance, a gap the regulator itself has acknowledged even as it has stopped short of mandating that insurers close it through binding product requirement.

5. REGULATORY FRAMEWORK: IRDAI GUIDELINES ON CYBER INSURANCE AND FRAUD MONITORING

The Insurance Regulatory and Development Authority of India has developed cyber insurance policy through a series of guidance documents addressing both product structure and institutional cybersecurity obligation. The IRDAI's Guidance Document on Product Structure for Cyber Insurance, issued on 8 September 2021, specifies that an individual cyber insurance policy should cover theft of funds arising from compromise of bank account, card or mobile wallet, third-party claims arising from identity theft, compromise of personal social media accounts, cyberstalking and data restoration cost following malware-induced loss, together with financial loss and defence cost arising from phishing attack, unauthorised online transaction, defamation or privacy-invasion claims arising from published digital content, and cyber extortion.[8] The Guidance Document further directs that claims below five thousand rupees may be supported by an electronic complaint filed with the National Cyber Crime Reporting Portal rather than a formal First Information Report, while confirming that a First Information Report remains a significant factor in assessing larger claims and cannot be dispensed with entirely; it recommends expanding standard coverage to address card cloning, SIM-jacking and skimming, presently underserved by the market despite constituting a significant source of loss in India, while confirming that damage to computer hardware and losses arising from ordinary commercial non-performance, such as failure to receive goods purchased online, fall outside conventional cyber-coverage.[9] Reflecting the Reserve Bank of India's zero-liability framework for unauthorised electronic transactions, customer liability is generally limited where the customer promptly reports an unauthorised transaction, typically within three working days of notification, with liability shifting to the bank

[8] Insurance Regulatory and Development Authority of India, Guidance Document on Product Structure for Cyber Insurance (Sept. 8, 2021).

[9] Id.

thereafter where neither party is directly responsible for the underlying system failure.[10]

IRDAI's cybersecurity governance framework has developed in three principal phases. The 2017 Guidelines on Information and Cyber Security for Insurers addressed multi-layered data protection, network-layer security and the role of security audit in identifying institutional cyber vulnerability.[11] These Guidelines were substantially expanded in 2022 to extend compliance obligation beyond insurers themselves to intermediaries, brokers, agents, third-party service providers, insurance repositories and surveyors.[12] This 2022 expansion reflected a considered regulatory judgment that insurer-level cybersecurity obligation alone could not adequately protect policyholder data given the sector's heavy reliance on an extended network of intermediaries and service providers, each handling sensitive personal and financial information at various points along the insurance value chain; a cybersecurity framework confined to insurers alone would, on this reasoning, have left precisely the weakest links in that chain outside direct regulatory reach.

The IRDAI Information and Cyber Security Guidelines, 2023 consolidated and refined this framework further, mandating risk-based assessment, continuous monitoring and organisational due diligence against contemporary cyber threat including data theft, identity theft and piracy, requiring independent annual assurance audit reported to IRDAI within a defined timeline, though the Guidelines' treatment of data classification remains insufficiently explicit regarding the consequence of classification breach, an ambiguity this paper's analysis in Part 6 identifies as a priority area for reform.[13] The 2023 Guidelines direct insurance entities to adopt best practice through self-certification prior to the discharge or determination of any contract, reinforcing accountability through the requirement that such self-certification be validated by independent assurance audit conducted on an annual basis and reported to IRDAI in a time-bound manner; this dual mechanism, self-certification supplemented by independent external verification, reflects an evident regulatory recognition that self-assessment alone cannot be relied upon to produce accurate cybersecurity compliance reporting, particularly given the commercial incentive an insurer may otherwise have to understate its own vulnerability.

---

10 Id.

11 Insurance Regulatory and Development Authority of India, Guidelines on Information and Cyber Security for Insurers (Apr. 7, 2017).

12 Insurance Regulatory and Development Authority of India, Guidelines on Information and Cyber Security (Sept. 2, 2022).

13 Insurance Regulatory and Development Authority of India, Information and Cyber Security Guidelines, 2023 (Apr. 24, 2023).

Most recently, the IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025, issued on 9 October 2025 and effective from 1 April 2026, replace the 2013 circular that had previously governed fraud monitoring and establish a substantially more comprehensive governance architecture, mandating a board-approved anti-fraud policy reviewed at least annually, a dedicated Fraud Monitoring Committee headed by key management personnel, and an independent Fraud Monitoring Unit.[14] The 2025 Guidelines classify fraud into internal, distribution-channel, policyholder or claims, external, and affinity or complex fraud categories, extend compliance obligation across the full distribution chain including corporate brokers, web aggregators, bancassurance partners, motor garages, hospitals and individual agents, and introduce a red-flagging mechanism for accounts under suspicion alongside an early-warning-signal framework intended to enable real-time incident response.[15] The extension of compliance obligation to motor garages and hospitals specifically is worth noting, since it reflects regulatory recognition that a significant proportion of policyholder and claims fraud originates not from the insurer or the policyholder directly but from third-party service providers, repair garages inflating motor-claim estimates or hospitals overstating treatment cost, whose fraudulent conduct the insurer alone bears little practical capacity to detect without the kind of coordinated, sector-wide reporting obligation the 2025 Guidelines now impose.

The Guidelines further mandate participation in a fraud-monitoring technology framework operated by the Insurance Information Bureau, which will maintain a Caution Repository of blacklisted distribution channels, vendors and known fraud perpetrators, and require structured reporting including an Annual Fraud Monitoring Report within thirty days of financial year-end, quarterly reporting to the risk management committee, and immediate escalation of internal fraud to the audit committee.[16] This represents a marked institutional shift from the 2013 framework's comparatively basic reporting requirement toward a governance structure placing fraud prevention squarely at board level, and its explicit recognition of cyber and new-age fraud as a distinct reporting category reflects regulatory acknowledgment of the trend this paper has traced throughout. The Caution Repository model in particular mirrors mechanisms already familiar from India's credit information infrastructure, under which centralised blacklisting of known defaulters or fraudulent actors allows individual regulated entities to benefit from intelligence gathered across the sector as a whole rather than relying solely on their own internal detection capacity, a design choice that should, over time, meaningfully reduce the ability

---

14 Insurance Regulatory and Development Authority of India, (Insurance Fraud Monitoring Framework) Guidelines, 2025, Ref. IRDAI/IID/GDL/MISC/112/10/2025 (Oct. 9, 2025).

15 Id.

16 Id.

of a fraudulent distribution-channel actor to simply migrate from one insurer to another once detected by the first.

6. TOWARD INTEGRATED CYBER-INSURANCE GOVERNANCE: ANALYSIS AND RECOMMENDATIONS

The regulatory trajectory traced above demonstrates considerable institutional progress, yet a structural gap persists between IRDAI's insurance-specific cybersecurity and fraud framework and India's general data protection regime under the Digital Personal Data Protection Act, 2023. The 2023 Guidelines' data classification framework, noted above, lacks explicit consequence for breach of classification, and neither the 2023 Guidelines nor the 2025 Fraud Monitoring Framework Guidelines expressly cross-reference the Digital Personal Data Protection Act's own breach-notification and penalty architecture, leaving insurers to reconcile two parallel compliance regimes without clear regulatory guidance on their interaction. This fragmentation carries practical consequence beyond mere administrative inconvenience: an insurer confronting a genuine data breach must presently determine, often under considerable time pressure, whether that breach triggers reporting obligations under IRDAI's sectoral guidelines, the Digital Personal Data Protection Act's general breach-notification requirement, or both simultaneously, and must further determine whether the remedial and penalty consequences that follow under each regime are cumulative, overlapping or potentially inconsistent with one another, a question neither statutory scheme presently answers with the clarity a well-functioning compliance system requires.

Given the insurance sector's unusually data-intensive character, this paper recommends that IRDAI issue supplementary guidance expressly harmonising its cybersecurity and fraud-monitoring framework with the Digital Personal Data Protection Act's data-fiduciary obligations, including explicit cross-reference to that Act's breach-notification timeline and its Section 33 penalty structure, so that insurers face a single, coherent compliance obligation rather than two independently evolving regulatory tracks addressing substantially overlapping data-security concern. IRDAI should further mandate that every insurer designate an officer functionally analogous to the data protection officer the Digital Personal Data Protection Act's Section 10 contemplates, empowered specifically to coordinate cybersecurity, fraud-monitoring and data-protection compliance across the entity, and should require the Insurance Information Bureau's Caution Repository to interoperate directly with the broader data-breach reporting infrastructure the 2023 Act establishes, ensuring that fraud intelligence gathered under insurance-specific regulation and personal-data-breach intelligence gathered under general data protection law are not maintained in isolation from one another.

Beyond this central recommendation, three further measures would strengthen the framework this paper has examined. First, IRDAI should clarify, through amendment or supplementary circular, the precise consequence attaching to a breach of the data classification scheme the 2023 Guidelines establish, closing the ambiguity Part 5 identifies and ensuring that insurers face predictable regulatory consequence rather than uncertain discretionary response. Second, the product-structure gaps the 2021 Guidance Document itself acknowledges, particularly around SIM-jacking, card cloning and skimming coverage, should be addressed through a defined timeline for market development rather than left to insurer discretion indefinitely, given the demonstrated scale of loss these categories already generate in the Indian market. Third, IRDAI should consider whether the Fraud Monitoring Committee structure the 2025 Guidelines establish could usefully be extended, in a coordinating rather than duplicative capacity, to oversee cyber insurance product adequacy specifically, given the close practical relationship between an insurer's internal fraud exposure and the adequacy of the cyber insurance coverage it in turn offers to its own policyholders.

7. CONCLUSION AND SUGGESTIONS

A comprehensive cyber insurance policy, properly structured and regularly reviewed, materially reduces the risk of cyber-related loss, and the sector's transition toward a "better normal" of expanded remote working makes continued growth in both individual and corporate cyber insurance demand a near certainty. India's cyber law regime, anchored in the Information Technology Act, 2000 and its subordinate rules and supplemented, where necessary, by the offence provisions of the Bharatiya Nyaya Sanhita, 2023, nonetheless remains imperfectly matched to the pace and variety of contemporary cyberattack, and the steady rise in cybercrime accompanying India's digital transformation confirms that legal and regulatory response must continue to evolve rather than treat the present framework as settled. The principle of good faith and the fiduciary character of the insurer-insured relationship, discussed in Part 2, remain the foundational commitments any cybersecurity or fraud-monitoring reform must ultimately serve: unauthorised access to policyholder data, wherever it originates within the insurance value chain, erodes the trust on which the entire insurance relationship depends, increases the transaction cost of insurance business, and generates precisely the vulnerability to further fraudulent practice this paper has traced throughout.

Under the present digital conditions, data protection, data integrity and data recovery following breach or manipulation constitute genuinely sensitive institutional objectives for every insurance entity seeking to maintain a resilient cyber environment. It is accordingly essential that IRDAI continue to revise its cybersecurity governance and cyber-resilience strategy in the interest of

insurers, insured parties and intermediaries alike, extending the institutional progress traced from the 2017 Guidelines through the 2023 Guidelines to the 2025 Fraud Monitoring Framework toward the closer integration with India's general data protection law this paper's recommendations in Part 6 propose, so that the insurance sector's considerable exposure to cyber-enabled fraud is met with a correspondingly coherent and comprehensive regulatory response. The trajectory this paper has traced, from a 1938 statutory framework built around the ordinary requirements of contractual good faith to a 2025 governance architecture addressing artificial intelligence, deepfakes and coordinated distribution-chain fraud, illustrates both how far Indian insurance regulation has travelled and how much further genuine integration between sectoral and general data protection law still requires it to go before India's cyber-insurance governance can be regarded as truly comprehensive.

BIBLIOGRAPHY

Reports and Secondary Sources

1. IRDAI-NHA Joint Working Group, Report of Sub-group on Fraud Control (Insurance Regulatory and Development Authority of India, 2019).
2. World Economic Forum, The Global Risks Report 2017 (12th ed. 2017).
3. IBM Security, Cost of a Data Breach Report 2021 (2021).
4. Risk Based Security, Q1 2020 Data Breach QuickView Report (2020).
5. Munich Re, Cyber Insurance: Risks and Trends (Apr. 2020).
6. Monalisha Mohanty, An Insight into Insurance Fraud and Its Prevention, 8(1) J. Ins. Inst. India 19 (2020).
7. Insurance Regulatory and Development Authority of India, Guidelines on Information and Cyber Security for Insurers (Apr. 7, 2017).
8. Insurance Regulatory and Development Authority of India, Guidelines on Information and Cyber Security (Sept. 2, 2022).
9. Insurance Regulatory and Development Authority of India, Information and Cyber Security Guidelines, 2023 (Apr. 24, 2023).
10. Insurance Regulatory and Development Authority of India, Guidance Document on Product Structure for Cyber Insurance (Sept. 8, 2021).
11. Insurance Regulatory and Development Authority of India, (Insurance Fraud Monitoring Framework) Guidelines, 2025, Ref. IRDAI/IID/GDL/MISC/112/10/2025 (Oct. 9, 2025).

Cases

1. Mithoolal Nayak v. Life Insurance Corp. of India, A.I.R. 1962 S.C. 814 (India).
2. P.J. Chacko v. Chairman, Life Insurance Corp. of India, A.I.R. 2008 S.C. 425 (India).
3. Syed Asifuddin v. State of Andhra Pradesh, 2005 Cri. L.J. 4314 (India).

Statutes

1. The Insurance Act, No. 4 of 1938, § 45 (India).
2. The Information Technology Act, No. 21 of 2000, § 2(1)(i) (India).
3. The Digital Personal Data Protection Act, No. 22 of 2023, §§ 10, 33 (India).
4. The Bharatiya Nyaya Sanhita, No. 45 of 2023 (India).
5. IRDA (Preparation of Financial Statements and Auditors' Report of Insurance Companies) Regulations, 2002 (India).