INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

"CYBER SECURITY INSURANCE IN INDIA: BRIDGING CORPORATE GOVERNANCE GAPS IN DIGITALLY VULNERABLE ECONOMY"

AUTHORED BY - BAVADHARANI U
LL.M (Student)
School Of Excellence In Law, TNDALU

ABSTRACT

The rapid advancement of technology in India has not only increased the volume of cyber risks but also expanded the threat landscape, revealing significant weaknesses in corporate governance. Even the recently enacted Digital Personal Data Protection Act, 2023, is not yet in effect. In this unpredictable digital economy, cyber insurance can serve as a strategic approach to safeguard companies against internet-related risks, particularly those tied to information technology infrastructure and its associated activities. First-party losses refer to direct financial damages that a company faces due to issues like data destruction, hacking, extortion, denial of service, ransom attacks, and liability coverage that compensates corporations for their losses. On the other hand, third-party losses involve costs incurred to reimburse partners or customers affected by a cyber breach. Without cyber security insurance, companies may experience lengthy recovery processes from hackers, leading to delays in compensating stakeholders and ultimately resulting in a loss of trust and privacy violations. Government initiatives, such as CERT-IN audits and the Cyber Crisis Management Plan (CCMP), aim to enhance cyber resilience. Given this context, this paper will explore the significance of implementing a robust cybersecurity policy in India.

KEYWORDS: cybersecurity insurance, malware, digital economy and corporate governance.

INTRODUCTION:

The growth of India's digital economy has really changed the way businesses operate, how governments function, and how people connect with one another. With the rise of platforms like the Unified Payments Interface (UPI), Aadhar-enabled services, digital medical records, and various e-commerce transactions, business activities have become more susceptible to

ISSN: 2582-6433

cyber-attacks. These cyber threats can be categorized into different types: offenses against individuals, which include corporate identity issues; offenses against property, which cover Intellectual Property Rights; and offenses against the government, such as cyber terrorism. This rapid digital transformation poses a significant risk, leading not only to the potential downfall of individual businesses but also to a loss of consumer trust and the stability of India's financial and commercial systems. In this context, Cyber Security Insurance has become an essential tool for managing risk. Unlike traditional insurance that typically addresses physical or financial losses, cyber insurance specifically covers losses resulting from digital incidents, including data breaches, system outages, regulatory fines, and damage to reputation. And in India the existence of cybersecurity insurance is in nascent stage with highest expected penetration in financial institutions and banks due to Reserve Bank of India (RBI)[1] and Insurance Regulatory and Development Authority of India (IRDAI)[2] but it also potentially needs it expansion in other critical infrastructure including healthcare, manufacturing, IT services and other business organisations.

When it comes to Cyber Insurance, it's not just about shifting risk; it plays a vital role in enhancing corporate Governance too. Insurers often require companies to implement security controls and incident response plans to qualify for coverage. This nudges organizations to raise their standards of transparency, accountability, and compliance with regulations. As a result, Cybersecurity insurance becomes an essential tool for addressing governance gaps. With India aiming to create a robust $1 trillion digital economy by 2030[3], bridging these governance gaps through effective cyber insurance frameworks is more important than ever.

Thus, this paper evaluates the role of cybersecurity insurance as public policy instrument over private just being private contract and proposes strategies for expanding its effectiveness across diverse sectors.

[1] PTI. (2017, February 19). *Banks look for insurance as cyber threats increase. The* Indian Express. https://indianexpress.com/article/india/banks-look-for-insurance-as-cyber-threats-increase-4532504/
[2] Gomathi, S. (2023). A study on data theft related to cyber offences in society. International Journal of Research Publication and Reviews, 4(1), 1416–1423. ISSN 2582-742.
[3] The Hindu Bureau. (2024, February 21). *DPIs to help India achieve $1 trillion digital economy by 2030*. *The Hindu*. https://www.thehindu.com/business/dpis-to-help-india-achieve-1-trillion-digital-economy-by-2030/article67871914.ece

ISSN: 2582-6433

2. NEED FOR CYBERSECURITY INSURANCE:

NOTPETYA ATTACK:

On June 2017, Small Computer Security Company called Linko's Group is the first Victim of this Malware. Not Petya is the most devasting variant of malware in history. The impact felt in Ukraine and its effect felt in many areas of globe. The Success of this attack commenced from release of Exploiting Malware called Eternal Blue and the vulnerability in Windows System. Eternal Blue in Conjunction with Hacking tool called Mimikatz, an open sources exploitation tool pushed the malware via a malicious update in M.E. Doc Software used to gather information and login Credentials of targeted Systems by exploiting the Server Message Block. This combination of this allowed widespread spread of Petya[4].

EFFECT:

M.E. Doc Software is a go-to for small businesses handling their accounting needs. Unfortunately, Not Petya acted like a ransomware attack, encrypting the entire target system and demanding victims pay a ransom in Bitcoins to regain access to their files. The problem is, it often damaged system data beyond the point of recovery. The malware made it impossible for victims to retrieve their credentials, leading them to believe they could decrypt their data after paying the ransom. This situation eroded trust in corporations and other stakeholders due to inadequate security measures. Not Petya impacted over 300 companies, including 22 banks, 6 power companies, 2 airports, 4 hospitals, and several government agencies in Ukraine, spreading its reach to around 65 countries and causing an estimated $10 billion in damages. It took weeks for business operations to get back to normal[5].

NEED:

In this Current Scenario, if business entities had Cybersecurity Insurance, it would have prevented companies could access quick recovery funds, helping them restore operations faster and could have prevented layoffs, bankruptcy, and collapse of small & medium enterprises (SMEs) and it would have prevented Government to bear complete cost of recovery and subsequently strengthen the resilience on digital economy by the tax payers.

[4] Schram, G. (2021, June 14). *Not Petya: Its consequences*, https://www.cybrary.it/blog/notpetya-its-consequences
[5] Ibid.

ISSN: 2582-6433

CYBERSECURITY INSURANCE PERILS AND COVERAGE:

Cybersecurity Insurance is essentially a policy crafted to shield the insured from cyber-related offences. To break it down a bit more, you can think of Cybersecurity Insurance as a risk management and mitigation strategy that not only helps in managing risks but also offers preventive measures. This, in turn, enhances the cybersecurity posture of organizations and, ultimately, benefits the country as a whole.

KEYSTAKEHOLDERS:

1. Insured or First Party: A client contacts their broker to purchase a policy and also engages a tech provider for a cyber evaluation.
2. Broker: A broker plays a crucial role in the buying process by assessing and quantifying risks. They offer recommendations on which insurance carriers to contact for quotes and help secure better premiums. Additionally, the broker encourages the buyer to collaborate with a tech provider for a thorough cyber evaluation.
3. Carriers (Insurance Service Provider): It's important to send a risk assessment questionnaire to the buyer and hire a third party to conduct a cyber risk assessment. This will help evaluate the reasonable risk management measures that the Corporation has in place, and ultimately, provide accurate quotations.
4. Reinsurers: Takes risk of the primary carrier[6].

COVERAGE:

First Party Coverage:

Loss on E-Threat:

In today's digital landscape, one of the biggest concerns is the threat of hackers. They can infiltrate the systems of organizations encrypting the sensitive data and important credentials, and then demand a ransom to unlock it. This is where Cybersecurity Insurance comes into play, helping to cover the losses faced by those insured[7].

Loss on E-Theft:

This happens when unauthorized or fraudulent data is entered into the system, often due to hacking or a breach in the insured system. This can lead to fraudulent fund transfers, resulting

[6]Data Security Council of India. (2023). Cyber Insurance in India [PDF]. Retrieved from https://www.dsci.in/files/content/knowledge-centre/2023/Cyber%20Insurance%20In%20India-doc.pdf

[7] Patil, A. A. (2024). Research paper on cyber security challenges and threats. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 4(1). ISSN 2581-9429.

ISSN: 2582-6433

in a financial loss for the insured party[8].

Loss Due to Fraudulent E-Communication:

For example, if the insured sends a fraudulent email to a customer with the intent of extorting money, the unsuspecting customer may believe the email is legitimate and transfer funds. Any financial loss incurred in this way would be covered under a Cybersecurity policy[9].

Loss Occurred due to Cyber Vandalism:

If the system or Internet of Things (IoT) is compromised and vandalized, leading to damage to the insured's computer, server, storage devices, or network systems with malicious intent, the Cybersecurity policy will assist in restoring or reconstructing these systems and any records that have been erased, distorted, or misled due to such vandalism.

Loss due to E-Business Interruption:

For Instance, E-Commerce platforms Network System can run slow due to exploration to cyber-attack and results in loss of customer, net profits and net expenses that are acquired on daily run business activity such damages are covered under E-Business Interruption.

Third Party Coverage:

Disclosure Liability Cost:

This includes legal expenses and compensation that must be paid to third parties in the event of a data breach that results in the public dissemination of critical information due to a cyber-attack. This encompasses information that has been outsourced to contractors, sub-contractors, vendors, and other third parties[10].

Conduit Liability:

Imagine a scenario where a service provider offers technology-based services, including applications and cloud-related software, to its customers. If such software is exploited and causes damage to third-party systems, Cybersecurity Insurance will cover the costs associated with the affected systems due to the insured software, which is the responsibility of the carriers under conduit liability. This also includes damages from hacking attacks or viruses[11].

Impaired Access Liability:

This covers situations where a Denial of Access (DOS) or Distributed Denial of Access

[8] Vaishavi, M., & Ameer, S. (2024). Data theft as emerging crime in India. *Journal of Emerging Technology and Innovative Research,* 11(7), ISSN-2349-5162

[9] Ghosh, S. (2023). Email spoofing detection. *IJARIIE, 9*(1). ISSN 2395-4396.

[10] Qian. (n.d.). *Cyber liability insurance policy: Coverage, benefits, cost, providers, companies and claims*. Retrieved [6th October, 2025], from https://www.qian.co.in/buy-cyber-liability-insurance-policy/

[11] Ibid.

ISSN: 2582-6433

(DDOS) attack disrupts the insured party's system, making it difficult for premium clients to access the website. As a result, any damages or losses suffered by third parties are included in the coverage[12].

Content Liability:

Cover losses incurred on Intellectual Property infringement like company patent or Trademark. For example, if the insured party a licensee had kept the Patent holder sensitive patent details in its system database and it became subjected to cyber-attack resulting in publication of such sensitive information in public. As the result the patent holder can hold the licensee liable for such breach for compensation. The defence cost and compensation to be paid on such breach are covered[13].

Reputational Liability:

For instance, electronic medical records or health records of an individual disseminated due to cyberattack on the insured critical infrastructure database which negatively impacted the reputation of the client such defence cost on defamation whether libel or slander can be claimed under the cybersecurity insurance.

Other Coverages:

It includes forensic cost necessarily to identify the offender and Notification cost that are incurred to inform the clients about the compromise of credential, credit monitoring cost[14].

ASSESSMENT OF RISK:

When it comes to cyber insurance in India, there are several key factors to consider. These include the internal incident repository, media information on cyber events and their outcomes, the firm's turnover, the territory and jurisdiction coverage needed, the required coverages, prior claims experience, and the industry the firm operates in. The process typically begins with filling out a proposal form and providing some supporting documents. After that, insurers usually conduct a thorough physical and technical assessment of the applicant's IT infrastructure. Generally, the journey starts with the insured party whether it's an individual or a business reaching out to an insurance broker or going directly to an insurance carrier[15]. The

[12] Impact of technological advances on insurance sector: A study on cyber insurance India. (n.d.). *Indian Journal of Integrated Research in Law*, 4(3), 899. ISSN 2583-0538.
[13] Qian. (n.d.). *Cyber liability insurance policy: Coverage, benefits, cost, providers, companies and claims*. Retrieved [6th October, 2025) from https://www.qian.co.in/buy-cyber-liability-insurance-policy/
[14] Gupta, C. (2024, December 11). *Understanding cyber insurance in India*. https://www.plumhq.com/blog/cyber-insurance-in-india
[15] Khalili, M. M. (2019). Embracing and controlling risk dependency in cyber-insurance policy underwriting. *Journal of Cybersecurity, 5*(1), 5.

ISSN: 2582-6433

broker serves as an essential middleman, guiding clients through the buying journey and helping them understand and evaluate their cyber risks. It's quite common for brokers to recommend involving a technology service provider to conduct a thorough cyber risk assessment. This assessment focuses on identifying any vulnerabilities in the insured's digital infrastructure and suggesting improvements if necessary. After this evaluation, the broker sends a risk assessment questionnaire to the potential policyholder, requesting detailed information about their business continuity plans and current cybersecurity practices. Occasionally, third-party cyber risk assessments are also commissioned to provide an impartial view of the insured's risk profile. Once all the relevant information is collected, the broker reaches out to different carriers for quotes, allowing the insured to compare coverage options and premiums[16]. The insured then picks the policy that fits best, weighing the coverage level, premium costs, and any extra services like incident response support or cybersecurity training. Finally, once everything is settled, the policy is issued, and the insured receives documentation that lays out the terms, coverage limits, exclusions, and how to file claims[17].

REGULATORY AND LEGAL FRAMEWORK AND IMPORTANCE IN COMPANIES:

INSURANCE ACT, 1938: The Indian government has placed a strong emphasis on securing the digital sector. To help with this, the Malhotra Committee introduced the Insurance Regulatory and Development Authority of India (IRDAI). Often referred to as the insurance watchdog of India, IRDAI plays a crucial role in safeguarding insurance companies against cyber threats. It establishes rules and guidelines to ensure these companies protect sensitive information, such as policy details and personal data. In 2020, the Insurance Regulatory and Development Authority of India (IRDAI) set up a working group focused on cyber insurance for institutions. The guidelines from IRDAI assist insurance companies in understanding how to evaluate and manage cyber risks, as well as outlining steps to take in the event of a cyberattack[18].

INFORMATION TECHNOLOGY ACT, 2000: The Information Technology Act, 2000 (IT

[16] Impact of technological advances on insurance sector: A study on cyber insurance India. (n.d.). Indian Journal of Integrated Research in Law, 4(3), 899. ISSN 2583-0538.
[17]Institute for Development and Research in Banking Technology. (2017). *Cyber insurance: A reference guide* https://www.idrbt.ac.in/wp-content/uploads/2022/07/CIFB.pdf
[18] Royan Jain, The Applicability of the Insurance Act 1938, In India: A Critical Analysis of Judicial Interpretation, International Journal on Creative Research Thoughts, Volume 12, Issue 4 April 2024.

ISSN: 2582-6433

Act) acts as the cornerstone for tackling cybercrime and managing digital governance in India. While it doesn't outright mandate cyber insurance, it lays down the legal foundations for the liabilities that such insurance typically covers. For example, Section 43A holds companies accountable if they fail to protect personal data, and if there's a data breach due to inadequate cyber security, it could result in legal action, tarnished reputation, and hefty fines. Moreover, Sections 70 and 72 delve into privacy violations, and Section 66A deals with offences related to emails. In this context, cyber insurance can play a crucial role in mitigating those risks.

NATIONAL CYBERSECURITY POLICY, 2013: The mission of the policy is to protect citizens, businesses and government to have secure cyber ecosystem by protecting information infrastructure, reducing vulnerabilities and minimise damage from cyber incidence. The root of Cybersecurity insurance can be traced from this policy. One of the strategies that was adopted in this policy is to create assurance framework[19].

DIGITAL DATA PROTECTION ACT, 2023: The Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant advancement in India's approach to data governance and privacy. This legislation was introduced to address growing concerns about the misuse and unauthorized access to personal data in our ever-evolving digital landscape. It lays out a comprehensive framework for the protection, processing, and management of digital personal data. Unlike the previous guidelines established in the Information Technology Act, 2000, which offered only limited and sector-specific privacy protections, the DPDP Act introduces a unified, rights-based legal framework that aligns with international standards, such as the EU's General Data Protection Regulation (GDPR). Yet, it also incorporates a distinctly Indian viewpoint, focusing on the rights of the "Digital Nagrik" and striving for more straightforward governance[20]. Data fiduciaries are now required to implement reasonable security measures to protect against data breaches, unauthorized access, or misuse. In the event of a data breach, the Act mandates that the Data Protection Board of India be notified, and when necessary, the affected individuals should also be informed. Furthermore, the Act empowers the government to exempt certain data fiduciaries from specific obligations, which has led to a mix of support for increased operational flexibility and concerns about potential accountability gaps.

[19] Impact of technological advances on insurance sector: A study on cyber insurance India. (n.d.). *Indian Journal of Integrated Research in Law*, 4(3), 899. ISSN 2583-0538.
[20] Kakkar, L. (2023, August 23). *Decoding the Digital Personal Data Protection Act, 2023*. EY India. https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023

ISSN: 2582-6433

This initiative enhances the collaboration between the public and private sectors by fostering interoperability. It strengthens both national and sectoral mechanisms, boosts ICT capabilities, and safeguards critical infrastructure for processing, handling, and transmitting sensitive data. Additionally, it encourages a regulatory framework for both in-house and outsourced security teams, supports cloud computing, fortifies encryption, and offers financial incentives for small and medium-sized enterprises while promoting research and development. It's a corporate responsibility to advocate for good governance by reinforcing security standards through firewalls and data protection tools, along with cybersecurity insurance, which paves the way for a more secure future. And such premiums and claims shall be disclosed by directors in every Annual General Meeting to ensure confidence to stakeholders that institution have financial backing in case of cyber incidents. Even, RBI mandates banks to adopt cyber risk frameworks includes cyber insurance could be integrated into compliance.

CONCLUSION AND SUGGESTION:

The digital economy has really changed the game for corporate governance in India. With cyber threats becoming more common and advanced, sticking to traditional governance methods just isn't going to cut it anymore. That's where Cyber Security Insurance (CSI) comes into play; it's a crucial tool for managing risks and enhancing corporate governance, fostering accountability, transparency, and financial resilience. While India has made progress with regulations like the IT Act, 2000 and the DPDP Act, 2023 and various sector-specific guidelines, the adoption of Cyber Security Insurance remains surprisingly low. This is mainly due to a lack of awareness, worries about costs, and not enough actuarial data. On the bright side, looking at global trends, it's evident Cyber Security Insurance can be a vital part of responsible governance, protecting shareholders that, customers, and critical infrastructure.

The suggestions include:

- First off, we should create a National Cyber Insurance Framework with the support of IRDAI and CERT-in.
- It's essential to require companies to disclose their Cyber Security Insurance coverage in their annual reports and SEBI governance filings to enhance accountability and build trust.
- Offering tax deductions or credits on Cybersecurity Insurance premiums could be particularly beneficial for small and medium-sized enterprises (SMEs) and startups.