IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Insurance And The Legal Framework: Efficacy And Limitations

- FATIMA DIANA MERIL A

ABSTRACT

The rapid digital transformation of the banking sector has significantly increased vulnerability to cyber-attacks, data breaches, and technology-driven financial crimes. As traditional insurance products largely focus on physical assets and fail to adequately cover intangible digital risks, cyber insurance has emerged as an essential risk-mitigation tool for banks. This study examines the rising importance of cyber insurance in the Indian banking industry by analyzing the escalation of cyber threats, regulatory requirements, and financial implications associated with cyber incidents. It also evaluates the evolving cyber insurance market in India through a comparative assessment of policy structures offered by private insurers such as HDFC Ergo and Bajaj Allianz, and highlights the considerable untapped potential due to limited involvement of public sector insurers. Additionally, the study explores the growing necessity of cyber insurance for newly consolidated Public Sector Banks, which now operate with larger digital footprints and interconnected systems. The findings reveal that cyber insurance plays a critical role in enhancing cyber resilience, ensuring business continuity, and safeguarding customer trust in an increasingly digital financial ecosystem. Overall, the research concludes that adopting comprehensive cyber insurance coverage is no longer optional but a strategic imperative for Indian banks facing escalating cyber risks and expanding digital operations.

KEYWORDS: Cyber Insurance, Banking Sector, Cybersecurity, Data Breach, Risk Management, Digital Banking, Public Sector Banks, Cyber-attacks, Insurance Market, Regulatory Compliance, Business Continuity, Cyber Risk Mitigation.

INTRODUCTION

In the normal course of business, banks may suffer financial losses due to unforeseen events. Some of these events may fall within the bank's control, enabling preventive measures. However, several incidents remain beyond their control and are therefore unavoidable. Natural calamities such as fires, earthquakes, and floods fall under this category. Although not natural in origin, incidents like theft and robbery are also considered unavoidable risks. To mitigate potential losses arising from such events, banks typically rely on insurance solutions. Over time, the insurance industry has evolved and developed specialized products tailored to the needs of banks and other financial institutions.

Cyber fraud has emerged as a major and growing threat for various sectors, especially financial institutions like banks. While banks continuously strengthen their cyber security frameworks to detect and prevent cyber-attacks and reduce financial losses, no defence mechanism can offer complete protection. Therefore, transferring the residual risk through cyber insurance becomes essential.

Cyber insurance is still an evolving field. Banks and other insured entities must assess their insurance needs, including the extent of coverage required, affordable premium levels, essential policy clauses, and the overall scope of protection. Simultaneously, insurance providers must understand the specific risk profiles and expectations of banks to design and deliver appropriate cyber insurance products.

CYBER INSURANCE

Traditional business insurance policies typically focus on covering **tangible** assets such as computers, laptops, and other hardware. However, emerging risks have revealed a significant gap — electronic data is not always recognized as a tangible asset under such policies. Cyber insurance is specifically designed to address this gap.

As banks become more digitally interconnected and operate in a global environment, their exposure to cyber threats continues to rise. With the rapid growth of sophisticated cybercrime, insurance solutions must evolve to meet these new challenges. Like any other insurance product, cyber insurance aims to both reduce risk and ensure that affected parties receive adequate compensation.

Cyber insurance is a specialized product that offers comprehensive protection against both **third-party liabilities** and **first-party costs** arising from unauthorized access or misuse of a bank's electronic or physical data and software. These policies can also cover expenses and liabilities stemming from network disruptions, malware attacks, data theft, and cyber extortion.

Additionally, cyber insurance may include coverage for business interruption losses, customer notification requirements, and costs associated with regulatory inquiries or penalties following a breach — without requiring physical damage as a trigger, which is typically mandatory in property insurance policies. Therefore, when evaluating policy options, banks should ensure that the coverage adequately addresses these evolving cyber risks.

Cyber insurance is an insurance product designed to help businesses hedge against the potentially devastating effects of cybercrimes such as malware, ransomware, distributed denial-of-service (DDoS) attacks, or any other method used to compromise a network and sensitive data. Also referred to as cyber risk insurance or cybersecurity insurance, these products are personalized to help a company mitigate specific risks.

First-party coverage refers to insurance benefits that reimburse the organization for expenses it directly incurs as a result of a cybersecurity incident.

Third-party coverage protects the organization against legal liabilities, such as claims or settlements arising from damages suffered by external parties due to the organization's actions or negligence.

For instance, in the event of a data breach where customer information is stolen and exposed online, first-party coverage would support the organization in meeting immediate costs such as forensic investigations and system restoration. On the other hand, third-party coverage would apply if affected customers file lawsuits seeking compensation for the misuse or exposure of their personal data.

BENEFITS OF CYBER INSURANCE

Cybersecurity insurance generally provides first-party protection for losses arising from events such as hacking, data destruction, data theft, and cyber extortion. Many policies also include coverage for legal fees and other related costs. While specific terms can differ across insurers and plans, cyber insurance commonly addresses the following key areas:

- **Customer notification costs:** Businesses are legally obligated to inform customers when their personal data has been compromised. Cyber insurance can help cover the expenses involved in issuing these notifications.
- **Assistance with identity restoration:** The insurance may support efforts to help affected individuals recover and protect their personal identities after a breach.
- **Data breach incidents:** Policies typically cover security events where confidential information is accessed, stolen, or exposed without authorization.

- **Data restoration:** Cyber insurance can fund the recovery and restoration of data corrupted or lost due to a cyberattack.
- **System repair:** The costs of repairing or restoring damaged IT infrastructure are often included.
- **Ransomware payments:** If attackers demand a ransom to release blocked or encrypted data, insurance may provide financial support toward these payments. However, regulatory bodies often discourage paying ransoms to avoid incentivizing criminal activity.
- **Incident response and legal support:** Coverage may extend to legal expenses associated with regulatory violations, as well as the cost of hiring cybersecurity specialists and forensic experts to investigate and remediate the attack.
- **Third-party liability:** If business partners or other external parties suffer losses due to unauthorized access to shared business data, the policy may cover the resulting claims.

CYBER RISKS EXCLUDED FROM CYBER INSURANCE COVERAGE

Cyber insurance policies generally exclude incidents that are considered preventable or caused by negligence or internal errors. Common exclusions include:

- **Weak security practices:** If a cyber incident arises due to inadequate security controls, poor configuration management, or ineffective protective measures.
- **Previous incidents:** Any breach or security event that took place before the insurance policy was purchased.
- **Employee mistakes:** Losses resulting from human error on the part of the organization's staff.
- **Insider misconduct:** Situations where data is stolen or compromised by an employee or trusted internal individual.
- **Known vulnerabilities:** Breaches caused by the organization's failure to fix or mitigate previously identified security weaknesses.
- **System upgrades:** Expenses associated with enhancing or upgrading technology systems, such as improving network defences or hardening software applications.

CHALLENGES OF CYBER INSURANCE MARKET: -

• Less awareness about cyber insurance amongst buyers.

• Enterprises finding purchasing and claim processes of cyber insurance to be wearisome.

• Damages due to cyber extortion, reputational loss, and rapidly evolving data and privacy policies makes it hard to quantify breadth and adequacy of cyber insurance cover.

• Cut throat competition on premium amounts by insurance companies

RECENT CYBER ATTACKS IN INDIA

In 2025, India has witnessed a sharp rise in cyberattacks, exposing critical weaknesses in the nation's digital infrastructure. These incidents—ranging from major data breaches to advanced malware operations—have impacted key sectors such as government, finance, and healthcare. The increasing sophistication and frequency of these attacks emphasize the urgent need for stronger cybersecurity frameworks, awareness, and policy interventions. The following 20 major cyber incidents reflect the evolving threat landscape and the mounting challenge of protecting India's digital ecosystem:

1. Large-Scale Cyber Offensive After Operation Sindoor

More than 1.5 million cyberattacks were launched against Indian digital systems following the Pahalgam terror event. Seven Pakistan-aligned APT groups targeted critical sectors like government agencies, healthcare, and banking. While only about 150 attacks succeeded, attempts were made to breach systems through phishing, malware, and DDoS techniques. CERT-In issued real-time warnings and shared related IOCs with affected entities.

2. "Dance of the Hillary" Malware Campaign

A Pakistan-origin spyware named Dance of the Hillary spread via social media links, compromising personal devices. It captured confidential user information by exploiting weak app settings and system vulnerabilities. Alerts were issued by central agencies and Punjab Police.

3. Star Health Data Leak and Extortion

A hacker identified as "xenZen" leaked 7.24 TB of personal and medical data belonging to 31 million customers of Star Health. The attacker later threatened company executives, escalating the incident from data theft to criminal intimidation.

4. BSE Cybersecurity Warning

Following CERT-In intelligence on ongoing cyber threats from Pakistan, the Bombay Stock Exchange issued advisories to the BFSI sector about the risks of ransomware, supply-chain exploits, and DDoS disruptions, urging preventive measures.

5. Cyber Fraud Network Exposed in Bihar

A fraud syndicate with cross-border links operated over 200 one-time-use bank accounts to facilitate financial scams. The group was uncovered under Operation Sindoor, revealing sophisticated laundering methods tied to Pakistan-based operators.

6. Telangana Cybercrime Crackdown

A 10-day operation in Gujarat led to the arrest of 20 individuals— including a bank manager—who were running nationwide investment and job scam networks using mule accounts and forged credentials.

7. Hacktivist-Driven DDoS Surge

Hacktivist groups from Southeast Asia targeted over 100 Indian organizations, causing service disruptions to express political dissent. Although no data theft occurred, the attacks exposed substantial resilience gaps.

8. Ulhasnagar Municipal Corporation Website Breach

UMC's official site was defaced with religious content, causing temporary service outage. Integrity was compromised, though no citizen data was affected.

9. Nippon Life AMC Cyber Incident

A cyberattack disrupted online services and mobile app functionality at Nippon AMC. While no data loss was confirmed, operations were temporarily suspended for security isolation.

10. Indian Cyber Force Retaliatory Actions

The Indian Cyber Force claimed responsibility for breaching Pakistani institutions, including Habib Bank and the Federal Board of Revenue, in response to the Pahalgam attack.

11. Triple-Layer Attack on Financial Institutions

Multiple intrusions across banks, payment gateways, NSE, and BSE were detected. Attackers exploited outdated systems and weak APIs, with some activities linked to Pakistan-based APT36 and Team Insane PK.

12. APT36 Defence Espionage Campaign

The Pakistan-backed APT36 used spear-phishing emails containing Crimson RAT malware to infiltrate defence networks, aiming to extract classified information.

13. ICICI Bank Vendor Portal Compromise

A third-party vendor portal was infiltrated to harvest login details and probe internal systems. Anomaly detection tools contained the attack early.

14. Aadhaar Authentication DDoS Attempt

UIDAI systems faced a brief outage due to DDoS traffic targeting Aadhaar services. Integrity and confidentiality remained intact.

In 2025, India has witnessed a sharp rise in cyberattacks, exposing critical weaknesses in the nation's digital infrastructure. These incidents—ranging from major data breaches to advanced malware operations—have impacted key sectors such as government, finance, and healthcare. The increasing sophistication and frequency of these attacks emphasize the urgent need for stronger cybersecurity frameworks, awareness, and policy interventions. The

- zero-trust security principles
- enhanced public-private intelligence sharing
- skilled cyber workforce development

As India moves toward deeper digitization, building a resilient and secure cyber ecosystem becomes essential to safeguard national security, economy, and public trust.

15. DigiLocker API Abuse

Misconfigured authorization tokens enabled unauthorized access to limited user information. The vulnerability was quickly patched after detection.

16. DRDO Targeted Spear-Phishing Attack

Malicious PDFs sent to DRDO scientists aimed at exfiltrating sensitive data. Cybersecurity controls prevented deeper system compromise.

17. Central Bank of India Phishing Infrastructure Abuse

Fraudsters duplicated the bank's online interface, misleading customers into divulging credentials. Session replay attempts were detected and blocked.

18. AIIMS Delhi Ransomware Attempt (Recurring)

Attackers attempted a follow-up intrusion after the 2022 ransomware breach. The attempt was intercepted before execution.

19. Operation Bunyān al-Marsūs Alert

CERT-In flagged a Pakistan-sponsored APT campaign targeting India's OT and SCADA systems controlling critical infrastructure like energy grids and transport networks.

20. WazirX Crypto Exchange Breach

State-sponsored Lazarus Group exploited smart-contract weaknesses to manipulate wallet permissions and execute unauthorized withdrawals, temporarily halting cryptocurrency trading.

The surge in cyberattacks during 2025 reveals how India's rapid digital expansion is being paralleled by advanced adversarial threats. These incidents highlight the necessity for:

- stronger national cybersecurity frameworks
- rapid vulnerability management
- zero-trust security principles
- enhanced public-private intelligence sharing
- skilled cyber workforce development

As India moves toward deeper digitization, building a resilient and secure cyber ecosystem becomes essential to safeguard national security, economy, and public trust.

IMPORTANCE OF CYBER INSURANCE IN BANKING SECTOR

Cyber insurance has become essential for banks, offering a vital financial safety net against severe cyber-attacks. By covering losses from data breaches, business interruptions, and legal liabilities, it protects banks that manage large volumes of sensitive customer data — helping them avoid crippling financial fallout, reputational damage, and regulatory penalties.

- **Financial protection**: A robust cyber-insurance policy enables a bank to absorb heavy expenses arising from ransomware attacks, data breaches, or major service disruptions — without draining its own capital or reserves. For instance, after a 2024 breach affecting a large insurer and its clients, the entities involved agreed to a US $6 million (≈ ₹50.1 crore) settlement with affected customers and insurance companies. This demonstrates how the financial impact of cyber incidents can run into crores — underlining the need for insurance.
- **Reputation management**: A single breach can severely dent public trust in a bank. Insurance helps cover the costs of public-relations efforts, customer communications, and remediation — assisting in rebuilding credibility while the bank focuses on fixing underlying issues.
- **Legal and regulatory compliance**: In the era of data protection laws like the Digital Personal Data Protection Act, 2023, banks face strict obligations to safeguard customer data. Cyber-insurance can cover liabilities arising from data-protection violations, costs tied to customer-notification, regulatory investigations, and potential fines.
- **Incident response and recovery**: Cyber-insurance supports a swift and organized response by covering forensic investigations, system recovery, IT remediation, business-interruption losses, and — where permitted — ransom payments or extortion costs. In this way, it enables banks to resume operations more quickly and minimize disruption.
- **Safeguarding sensitive data**: Banks store vast amounts of personal and financial information. Since traditional property insurance often excludes "intangible" assets like data, cyber-insurance fills that crucial gap and provides a financial shield when sensitive data is compromised.
- **Complement to security infrastructure**: No matter how advanced a bank's cybersecurity tools — firewalls, encryption, intrusion-detection, access controls — real-world threats are increasingly sophisticated. Cyber-insurance acts as a fallback — a financial safety net recognizing that even the best defenses cannot guarantee absolute security.

CONCLUSION

With the rapid expansion of digital banking, cyber insurance has become a crucial protective mechanism for financial institutions to safeguard themselves against the rising threat of cyber-attacks. The growing demand for cyber insurance in India clearly reflects its increasing significance for the banking industry. The surge in cyber-incidents and major data breaches in recent years underscores the need for strong risk-transfer measures such as cyber insurance.

Furthermore, the recent mergers of Public Sector Banks, which have led to the creation of larger and more interconnected entities, heighten the need for advanced cyber-risk coverage to protect their expanded digital infrastructure. Comparative studies of cyber insurance offerings by companies like HDFC Ergo and Bajaj Allianz, along with an assessment of the cyber insurance markets in India and abroad, reveal substantial growth potential. The Indian market remains largely untapped, particularly because public sector insurers have yet to make a strong entry into this segment.

Therefore, the findings of this study indicate that cyber insurance is becoming critically important for the Indian banking sector. Increasing cyber-attack risks, evolving insurance products, and a growing market landscape collectively point toward cyber insurance emerging as an indispensable component of modern banking risk management in India.