International Journal of Academic Research
P-ISSN: 2348-7666: Impact Factor: 6.023
Homepage: https://www.ijar.org.in/
Volume-12, Issue-3(2), Jul-Sep-2025

A Study on Cyber Threat Challenges and Mitigation Strategies in Safeguarding General Insurance in the Digital Era

[1] Adarsha MPM and [2]Dr. Giridhar K. V
[1]Research Scholar, Sahyadri Commerce and Management College, Constituent College of Kuvempu University, Shivamogga
[2] Professor and Research Supervisor, Sahyadri Commerce and Management College, Constituent College of Kuvempu University, Shivamogga

Abstract:
Increasing cyber threats in the general insurance industry are also in line with the rapidly increasing digitization of processes and sensitive customer information handling. The risks are escalating as they include ransomware, phishing, data breach, and they all are combined with outdated systems, third-party dependencies, and low cyber awareness. This is why a multilayered cybersecurity framework (that includes technical controls, organizational controls, employee education and a solid incident-response approach) is the only way to diminish these threats. To ensure data safety, the maintenance of their functional continuity, and a sustainable trusting relationship created in the digital era, the emphasis on cyber resilience is necessary

Keywords: Cybersecurity, General Insurance, Digital Era, Cyber Threats, Risk Mitigation.

Introduction

The use of digital transformation in the general insurance business has significantly promoted business proficiency within the business, customer support capacity, as well as market expansion. Automated underwriting, policy servicing and claims handling have been automated through cloud computing, mobile platform, artificial intelligence (AI) and big-data analytics. On the other hand, this digitisation has also been characterised by increased sector sensitivity when it comes to the realm of cyber threats. Within the general insurance companies, massive amounts of critical personal and financial data are being managed nowadays and this made them the potential receiver of criminals in cyber space.

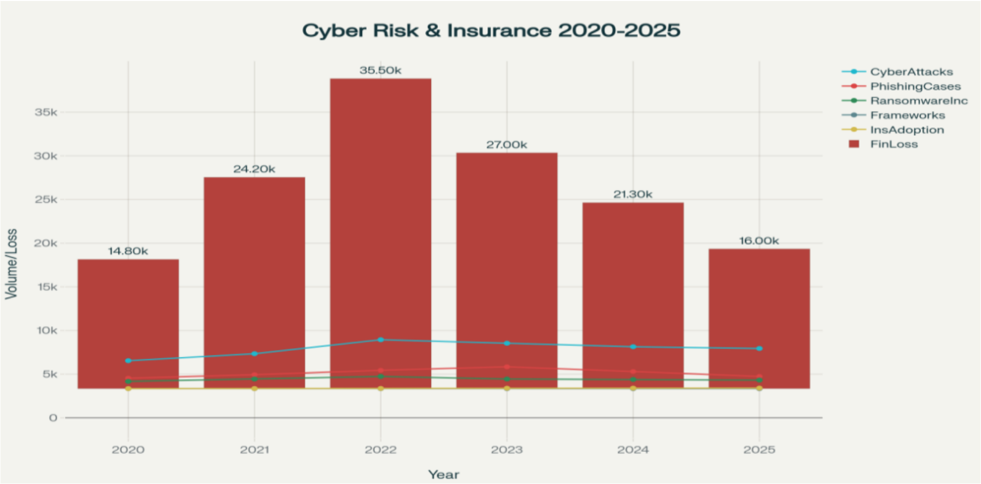
In response, cybersecurity has been developed as a precious tactic. According to the Cost of a Data Breach Report of IBM (2024), the average cost of data breaches in the financial-services industry is about $5.90 million, and the most frequent cause of data breaches is compromised credentials. Insurance as a part of financial services industry is one of the five most targeted industries in the world. In the Indian case, PwC (2023) reported that in the country, almost 70 percent of the insurers have reported attempted cyber-attacks within the last three years. That has triggered the Insurance Regulatory and Development Authority of India (IRDAI) to mandate an increase in the systems of data-security, cybersecurity testing, and incident management by insurers (IRDAI, 2022).

At the same time, new threats, such as ransomware attacks, phishing, malware injection, and DDoS (Distributed Denial of Service) attacks, have resulted in a significant loss of money and reputations of insurers on a global scale (McKinsey & Company, 2023). The risk environment has expanded due to the adoption of remote working behaviours and cloud-based IT infrastructure by insurers, and it is now important that the cybersecurity approach should be proactive and have multiple layers (Deloitte, 2023).

Cyber Threat Landscape in India

Cyber threats refer to malicious acts aimed at damaging, stealing, or disrupting digital systems, networks, or data. These include a wide range of activities such as hacking, phishing, malware attacks, ransomware, denial-of-service attacks, and insider threats. With India undergoing rapid digitization across industries, especially in financial services and insurance, the country has become increasingly exposed to cyber risks. The growing use of digital payments, cloud computing, mobile applications, and internet-based platforms has expanded the potential attack surface for cybercriminals.

India ranks among the top countries most targeted by cyberattacks globally. According to the Indian Computer Emergency Response Team (CERT-In), India reported over 1.39 million cyber incidents in 2022, a sharp increase from around 3.1 lakh cases in 2019, reflecting a compounded annual growth rate of more than 70% in just three years. The IBM X-Force Threat Intelligence Index (2023) placed India second in the Asia-Pacific region for the number of cyberattacks, with a significant proportion targeting sectors such as finance, insurance, healthcare, and government. These attacks include phishing, data theft, ransomware, and cloud misconfiguration exploits.



Source: IRDI Reports

Cyber Threat Landscape in General Insurance

The insurance sector is increasingly vulnerable to a variety of cyber threats due to the sensitive nature of the data it handles and the complexity of its IT infrastructure. Key cyber threats include:

Ransomware Attacks: Ransomware is malicious software that encrypts an organization's data, rendering it inaccessible until a ransom is paid. In the insurance sector, such attacks can halt policy issuance, claims processing, and customer service. Attackers often target backup systems to ensure maximum impact.

Data Breaches: Insurance firms collect and store vast amounts of personally identifiable information (PII), including names, addresses, medical histories, and financial details. Hackers target this information for identity theft, financial fraud, and resale on the dark web. A breach can result in severe legal and financial consequences.

Phishing and Social Engineering: Phishing emails and messages trick employees into revealing login credentials or clicking on malicious links. Cybercriminals often impersonate clients, agents, or even executives to gain unauthorized access to internal systems.

Supply Chain Attacks: General insurers rely on third-party vendors for services like document verification, digital onboarding, and payment processing. Vulnerabilities in these vendors' systems can be exploited to gain access to the insurer's network.

Insider Threats: Malicious or negligent actions by employees, such as mishandling data or sharing confidential information, pose internal risks. Insider threats are harder to detect as they originate from within the organization.

Distributed Denial-of-Service (DDoS) Attacks: These attacks flood online services with traffic, making websites and mobile apps inaccessible to legitimate users. Such disruptions can erode customer trust and delay operations.

KEY RISK FACTORS IN THE INSURANCE SECTOR

The insurance sector is increasingly vulnerable to cyber threats due to the nature of its operations and data. Several underlying risk factors heighten this susceptibility:

1. **Sensitive and Financial Data**: Insurance companies store vast amounts of personally identifiable information (PII), such as health records, financial data, social security numbers, and policy details. This type of data is highly attractive to cybercriminals for identity theft, financial fraud, and ransomware attacks.
2. **Legacy IT Systems**: Many insurance companies still operate on outdated and fragmented IT infrastructures, often due to years of mergers and acquisitions. These legacy systems lack the latest security protocols and are vulnerable to exploitation.
3. **Third-Party Dependencies:** The sector depends on multiple third-party service providers, including cloud vendors, software suppliers, and data processors. Each of these external partners poses a potential entry point for cyberattacks, especially if their own security standards are inadequate.
4. **Low Cyber Awareness Among Employees**: A significant portion of cybersecurity incidents stem from human error, such as clicking on phishing links or falling victim to social engineering. Inadequate cybersecurity training and awareness programs increase this risk.
5. **Complex and Evolving Regulatory Requirements:** Insurers must comply with a variety of local and global data protection regulations, such as GDPR, IRDAI cybersecurity guidelines (India), and others. The cost and complexity of compliance can overwhelm smaller firms and leave gaps in security policies.
6. **High Volume of Digital Transactions:** With increasing digitization, insurance companies now handle thousands of online transactions daily from claims processing to customer service. This creates a larger attack surface and raises the risk of transaction-based fraud and data breaches.
7. **Target for Ransomware**: Insurers are prime targets for ransomware attacks due to their financial resources and critical data. Cybercriminals may exploit vulnerabilities to encrypt critical data and demand large sums for decryption keys.
8. **Inadequate Incident Response Plans:** Many insurers still lack comprehensive incident response and disaster recovery plans. A delayed or uncoordinated response to

cyber incidents can amplify the damage and lead to significant financial and reputational loss.

MITIGATION STRATEGIES AND CYBERSECURITY FRAMEWORK

To safeguard digital operations and customer data, insurers must adopt a multi-pronged cybersecurity approach:

a) Technical Safeguards

To enhance cybersecurity in the insurance sector, companies should implement firewalls and endpoint security to safeguard devices and communication channels, use multi-factor authentication (MFA) for added login protection, and apply encryption to secure data both at rest and in transit. Leveraging AI-driven threat detection helps identify anomalies and potential breaches in real-time, while secure cloud storage with compliant providers ensures safe and reliable data management.

Firewalls and Endpoint Security
Multi-Factor Authentication (MFA)
Encryption
AI-Driven Threat Detection
Secure Cloud Storage

b) Organizational Policies

Effective cybersecurity requires strong governance through the appointment of a Chief Information Security Officer (CISO) to lead data protection efforts. Companies should also invest in cyber risk insurance to cover potential losses from cyberattacks. Regular compliance monitoring with standards like ISO 27001 and IRDAI guidelines ensures adherence to best practices and regulatory requirements

Cybersecurity Governance
Cyber Risk Insurance
Compliance Monitoring

c) Human Resource Measures

Enhancing cybersecurity involves employee awareness training through regular workshops to recognize phishing and fraud, implementing role-based access controls (RBAC) to restrict system access, and conducting regular security audits like penetration testing and vulnerability assessments to detect and address potential risks.

Employee Awareness Training
Access Management
Regular Security Audits

d) Incident Response and Recovery

A strong cybersecurity framework includes a Cyber Incident Response Plan (CIRP) to detect, respond to, and recover from attacks, backup and recovery systems with encrypted off-site backups and regular drills, and a Business Continuity Plan (BCP) to maintain essential operations during cyber crises.

Cyber Incident Response Plan (CIRP)
Backup and Recovery Systems
Business Continuity Plan (BCP)

Conclusion

In conclusion, the digital transformation of the general insurance sector has brought significant benefits in terms of efficiency, customer service, and scalability, but it has also exposed insurers to a complex and evolving landscape of cyber threats. From ransomware and data breaches to phishing attacks and insider threats, the risks are numerous and increasingly sophisticated. These threats are compounded by legacy systems, third-party dependencies, and low levels of cybersecurity awareness. To effectively safeguard operations and maintain customer trust, insurers must adopt a holistic cybersecurity framework that integrates technical safeguards, strong organizational policies, well-informed and trained employees, and a robust incident response and recovery mechanism. Proactive investment in cybersecurity infrastructure, continuous regulatory compliance, and a culture of cyber resilience are essential for ensuring long-term sustainability and protection in the digital era.

References

1. Deloitte. (2023). Global insurance outlook: Balancing growth, cost, and technology. Deloitte Insights. https://www2.deloitte.com
2. IBM Security. (2024). Cost of a Data Breach Report 2024. IBM. https://www.ibm.com/reports/data-breach
3. IRDAI. (2022). Guidelines on Information and Cyber Security for Insurers. Insurance Regulatory and Development Authority of India. https://irdai.gov.in
4. McKinsey & Company. (2023). Cybersecurity in insurance: Why insurers must up their game. https://www.mckinsey.com
5. PwC India. (2023). Insurance Sector Cybersecurity Trends in India. PricewaterhouseCoopers. https://www.pwc.in
6. ISO/IEC. (2022). ISO/IEC 27001: Information Security Management Systems – Requirements. International Organization for Standardization. https://www.iso.org
7. CERT-IN. (2023). Annual Threat Report 2023. Indian Computer Emergency Response Team. https://www.cert-in.org.in
8. NIST. (2020). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. https://www.nist.gov