13. Cyber security, cyber insurance and digital risk management

[1]Dr. R. Srikala, [2]V.Sanjeev Kumar

[1]Assistant Professor, Department of B.Com BPS,
Sri Ramakrishna College of Arts & Science, Coimbatore.
[2]Student, II-year, Department of B.Com BPS,
Sri Ramakrishna College of Arts & Science, Coimbatore.

Abstract

This document explores the critical need for evolving insurance frameworks to address increasingly systemic emerging risks, including global pandemics, large-scale cyber attacks, and heightened geopolitical instability. Traditional insurance models often struggle with the correlated nature of these threats, leading to significant protection gaps. The analysis proposes a shift toward innovative risk-sharing mechanisms, specifically highlighting public-private partnerships as a viable solution to enhance financial resilience and provide sustainable coverage for catastrophic, boundary-spanning events. The study specifically contextualizes these global challenges within the Indian insurance landscape, noting the urgent need for innovative solutions to bridge the nation's significant protection gap.By contextualizing these global challenges within the Indian insurance landscape, the study underscores the urgent need for a regulatory and operational transformation.

Introduction

The global insurance landscape is currently navigating a period of unprecedented volatility. Emerging risks, most notably systemic threats such as global pandemics, large-scale cyber attacks, and intensifying geopolitical instability, are redefining the traditional boundaries of insurable risk. Unlike conventional hazards, these threats exhibit high correlation, creating cumulative impacts that frequently exceed the capacity and risk appetite of private underwriting markets. As these protection gaps widen, the resilience of national and international economies faces significant pressure. This document examines the structural limitations of existing insurance frameworks in the face of these boundary-spanning events. Furthermore, it advocates for a fundamental shift toward collaborative risk-sharing mechanisms, with a particular emphasis on public-private partnerships (PPPs) as a strategic necessity. By contextualizing these challenges within the unique contours of the Indian insurance sector, this analysis highlights the urgent requirement for innovative, proactive frameworks capable of safeguarding financial stability in an increasingly uncertain global environment.

Cyber security

Cyber security is defined as the practice of protecting systems, networks, and programs from digital attacks. These cyber threats are typically aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes. In an increasingly interconnected global economy, cyber security is no longer merely an IT concern but has evolved into a critical pillar of institutional resilience, directly influencing an organization’s susceptibility to the systemic risks discussed in this document.

 ISBN: 978-81-687720-2-1

Cyber security insurance

Cyber security insurance is a specialized policy designed to offset the devastating financial impacts of cyber incidents. Comprehensive policies typically provide coverage for both first-party costs—such as forensic investigations, data restoration, and ransom demands—and third-party liabilities, including legal fees and regulatory fines.It is important to note that insurance cannot replace a robust digital risk management framework. Underwriters increasingly require organizations to maintain strict technical defenses, such as Multi-Factor Authentication (MFA), Endpoint Detection and Response (EDR), and tested backups, to obtain coverage or avoid claim denials. An effective digital risk management framework involves identifying, measuring, prioritizing, and mitigating digital threats through established risk registers, continuous vulnerability assessments, and strict Incident Response Plans.In the Indian market, several major insurers offer specialized cyber policies. For instance, HDFC ERGO provides policies for digital theft of funds, cyber extortion, and system restoration, while TATA AIG offers digital plans covering online fund theft, cyberbullying, and system data recovery.

Why you need cyber security insurance

As digital transactions, UPI usage, and remote work become standard, reliance on interconnected networks has increased your exposure to digital crimes. Traditional business liability or personal homeowners policies rarely cover digital incidents. Cyber insurance acts as a critical safety net to mitigate direct financial losses and help restore compromised data or reputations.Cybersecurity insurance is a vital financial safety net that shields your business or personal finances from the devastating costs of cyber incidents like data breaches, ransomware, and cyber fraud. Standard business or homeowners' policies do not cover these digital threats.

What It Covers

Cyber policies are generally divided into two main categories, plus additional specialized coverages:

First-Party Coverage: Direct costs your organization or household suffers during an attack. This includes data recovery, malware removal, business downtime losses, crisis management, and cyber extortion (ransom payments). First-party coverage in cyber insurance protects your business against direct financial losses caused by a cyberattack or data breach. It pays for your own recovery expenses, such as IT forensics, ransomware payments, data restoration, business interruption, and crisis management, rather than defending you against lawsuits filed by third parties. A robust first-party cyber insurance policy provides a critical safety net for the immediate expenses and long-term recovery costs following an incident. Key components typically include:

- Incident response & forensics
- Business interruption
- Data recovery
- Cyber extortion
- Notification & crisis management
- Funds transfer & fraud

 ISBN: 978-81-687720-2-1

Third-Party Coverage: Protection against lawsuits and regulatory fines if customer or employee data is compromised. This helps pay for legal counsel, customer notification services, and liability settlements.Third-party cyber insurance covers the legal costs, settlements, and financial damages your business faces if a client, partner, or customer sues you for failing to protect their data or causing a cyber-related incident.This coverage, typically known as Cyber Liability Insurance, is distinct from first-party policies (which pay for your own direct expenses like ransomware recovery or IT forensics).

Key areas usually covered under third-party cyber insurance include:

- Privacy & security liability
- Regulatory fines & penalties
- Media liability
- Vendor & partner liability

Cyber Crime: Protection against financial theft resulting from social engineering, identity theft, or unauthorized fund transfers.the landscape of cyber crime protection in cyber insurance is highly enhanced. Policies vary significantly based on whether you are looking
for personal or commercial coverage as well as the specific insurance provider.

Core Coverages

- Ransomware & Extortion: Covers the costs of negotiating and paying ransoms, as well as hiring IT forensics to restore systems.
- Social Engineering Fraud: Protects against deception scams (e.g., Business Email Compromise, fake vendor invoices) that manipulate employees into transferring funds.
- Data Breach & Identity Theft: Reimburses the costs of legally mandated customer notifications, credit monitoring, and PR crisis management.
- Theft of Funds: Covers direct losses if a cybercriminal gains unauthorized access to your personal or business bank accounts.

Importance of cyber security insurance

In an era of escalating digital reliance, cyber security insurance serves as a critical mechanism for institutional resilience. As systemic cyber threats increasingly bypass traditional risk boundaries, these specialized policies provide essential financial stability, shielding organizations from the catastrophic impact of data breaches and business interruption. Beyond pure risk transfer, such insurance often incentivizes the adoption of robust digital hygiene, ensuring that institutions remain proactive against emerging vulnerabilities while maintaining stakeholder confidence in the face of inevitable disruptions.

Key aspects

- Institutional Resilience: Serves as a vital mechanism for maintaining stability as systemic cyber threats increasingly bypass traditional risk boundaries.
- Financial Stability: Shields organizations from the catastrophic financial impacts caused by data breaches and business interruptions.
- Incentivizes Digital Hygiene: Encourages the adoption of proactive security measures, ensuring organizations remain vigilant against emerging vulnerabilities.

 ISBN: 978-81-687720-2-1

● Maintains Stakeholder Confidence: Provides assurance to stakeholders by demonstrating the capacity to withstand and recover from inevitable cyber disruptions.

Future of cyber security insurance

The future of cyber security insurance is defined by stricter, AI-driven risk profiling, mandatory cybersecurity maturity thresholds, and hyper-specialized policies that cover emerging threats like agentic AI vulnerabilities. Moving away from retroactive payouts, policies now heavily emphasize pre-breach resilience and dynamic premium adjustments.

The cyber insurance industry is shifting rapidly in several critical directions to adapt to escalating threats and a changing regulatory environment:

● Mandatory Security Thresholds: Underwriters no longer issue policies based on a simple application. Buyers must prove compliance with robust IT controls, such as mandatory Multi-Factor Authentication (MFA) for all remote access, tested Incident Response Plans, and active endpoint security (EDR/XDR).

● AI-Assisted Underwriting & Telemetry: Insurers use continuous, non-intrusive scanning and AI analysis of a company's IT environment to assess risk. Companies with stronger "cyber hygiene scores" can secure lower premiums.

● Emerging AI & Geopolitical Risks: Policies are evolving to address third-party losses, privacy violations, and business interruptions stemming from the use of agentic AI. Additionally, strict exclusions are being written for nation-state sponsored attacks and acts of war.

● Pre-Breach Partnerships: Insurers are increasingly partnering with cybersecurity firms to offer active threat monitoring, vulnerability scanning, and rapid incident response services as part of the policy package, making the insurer a partner in active defense rather than just a financial safety net.Market Stabilization: While premiums surged significantly in the early 2020s, the market has recently stabilized. However, high-risk sectors (such as healthcare) may still see rising costs due to claims severity. Growth of cyber insurance in india The cyber security insurance market in India is experiencing rapid, high-trajectory growth, projected to scale from around $580 million to over $5 billion in the coming decade, driven by surging ransomware attacks, expanding digital ecosystems, and strict new data privacy laws.

This growth is primarily propelled by several key market dynamics:

● The DPDP Act Impact: The implementation of the Digital Personal Data Protection (DPDP) Act has elevated the financial and reputational stakes for data breaches, compelling both large enterprises and MSMEs to secure liability coverage.

● Ransomware & Business Interruption: Data breach and ransomware coverages are the most in-demand segments, commanding an estimated 34% of the market as businesses face complex recovery and operational downtime costs.

● Tighter Underwriting: Driven by frequent malware and phishing incidents in the BFSI and e-commerce sectors, insurers have tightened guidelines, often requiring proof of strong cybersecurity hygiene (e.g., Multi-Factor Authentication, external attack surface scans) before issuing policies.

Growth chart

Digital risk management and insurance

Digital risk management and insurance are inextricably linked; insurance serves as the final, strategic layer of defense within a comprehensive cyber resilience framework, not a substitute for

 ISBN: 978-81-687720-2-1

operational security. Underwriters increasingly demand evidence of proactive risk management—such as rigorous vulnerability assessments, regular staff training, and the implementation of advanced security controls like EDR and MFA—as a condition for policy issuance. By integrating real-time telemetry and periodic risk audits into the underwriting process, insurers do more than provide financial protection; they actively incentivize organizations to maintain superior digital hygiene, thereby reducing the probability of claim-triggering events.

Steps to Claim a cyber security insurance

Filing a cyber security insurance claim in India involves notifying your provider immediately, filing a police First Information Report (FIR), and submitting formal proof of loss.

Settlements typically cover expenses like forensic investigation, legal defense, and data restoration.

Essential Steps to File a Claim

● Report the Incident Immediately: Contact your insurance provider (e.g., HDFC ERGO, Tata AIG, SBI General) within 24 to 48 hours. Many insurers provide specific customer portals or toll-free numbers.

● File an FIR: Lodge a formal complaint at your local police station or report the cybercrime online through the official National Cyber Crime Reporting Portal.

● Gather Documentation: Assemble all necessary evidence, including screenshots of the breach, the police FIR copy, bills for restoration, and any available forensic reports.

● Forensic Assessment: The insurer may appoint an investigator or external cyber expert to analyze the severity of the attack and assess the sustained financial damages.

● Claim Settlement: Once the insurer's claiming team reviews and approves the submitted documents and investigation report, the settlement will be processed according to your policy's terms.

Default of cyber security insurance

A default or rejection of a cyber security insurance claim happens when an insurer refuses to pay out for a cyber incident, such as a ransomware attack, data breach, or wire fraud. Over 40% of cyber insurance claims face denial, primarily because businesses fail to meet the strict prerequisites and conditions outlined in their policy fine print. The most common reasons underwriters default or deny cyber security claims include: Missing or Incomplete Security Controls: Insurers make coverage conditional on maintaining minimum defenses. If a breach reveals the business did not implement required Multi-Factor Authentication (MFA), Endpoint Detection and Response (EDR), or reliabledata backups, the claim is usually denied. Application Misrepresentation: If a company overstated its security posture (e.g., claiming MFA is enforced everywhere when it isn't) on the initial insurance application, the insurer can void the policy entirely.

Known Unpatched Vulnerabilities: Claims can be denied if the attack exploited a security gap or known vulnerability that the organization's IT team was aware of but failed to patch prior to the incident. Late Notice Clauses: Most policies require the insured to notify the carrier within a strict window, typically 48 to 72 hours. Delays in reporting can automatically invalidate the claim. Standard Exclusions: Losses stemming from deliberate insider attacks, acts of war, or the non-compliant gathering of data (e.g., violations of biometric privacy laws) are explicitly excluded from standard policies.

 ISBN: 978-81-687720-2-1

Global market of cyber security insurance

The global cybersecurity insurance market is valued at roughly $23 billion to $33 billion, with projections indicating explosive growth to over $220 billion by 2034. Driven by surging ransomware threats and strict data regulations, North America dominates the space, while SMEs (Small and Medium Enterprises) are the fastest-growing customer segment.

Conclusion

As systemic risks such as global pandemics, large-scale cyber incursions, and geopolitical volatility become increasingly intertwined, the traditional boundaries of insurable risk are being fundamentally redrawn. These boundary-spanning events often exceed the risk appetite and financial capacity of the private insurance market, creating significant protection gaps that threaten economic stability. To bridge these gaps, stakeholders must move beyond reactive models toward proactive, collaborative frameworks. The integration of public-private partnerships (PPPs) represents a critical structural evolution, ensuring that catastrophic risks are shared equitably and managed with greater resilience. Furthermore, in the digital domain, cyber insurance should no longer be viewed as a standalone financial product but as a strategic component of a broader risk management ecosystem. By mandating robust digital hygiene and incentivizing proactive threat mitigation, insurers can transform from mere risk underwriters into active partners in institutional resilience. As the Indian insurance sector navigates this trajectory—catalyzed by the Digital Personal Data Protection (DPDP) Act and an expanding digital economy—the adoption of these sophisticated, data-driven frameworks will be the defining factor in safeguarding financial stability in an increasingly uncertain global environment.

 ISBN: 978-81-687720-2-1