

## **185. Customer Trust and Adoption of Cyber Insurance Products in India: Challenges, Determinants and Future Prospects**

Dr.N.Srividya

Department of Corporate Secretaryship & Accounting and Finance, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamilnadu,India.

### **Abstract**

*The growth of digital payments, cloud computing, e-commerce and remote working has significantly increased cyber risks in India. Data breaches, ransomware attacks, phishing and identity theft have become major concerns for businesses and individuals. Cyber insurance has emerged as an important financial protection mechanism against such risks. Despite growing cyber threats, the penetration of cyber insurance in India remains low. This paper examines the role of customer trust in influencing the adoption of cyber insurance products in India. The study discusses awareness, insurer reputation, transparency, pricing, service quality and regulatory support as major determinants of customer trust and purchase intention. The paper concludes with strategic recommendations for insurers and policymakers to improve cyber insurance adoption and strengthen cyber resilience in India.*

**Keywords:** Cyber Insurance, Customer Trust, Adoption, Digital Security, India, Emerging Risks

### **1. Introduction**

India is among the fastest growing digital economies in the world. Digital banking, UPI transactions, online shopping and cloud-based business operations have transformed the way individuals and organizations operate. However, increased digital dependence has exposed customers and organizations to cyber threats. Cyber insurance provides financial protection against losses resulting from cyber incidents including data breaches, business interruption. Although awareness of cyber security has increased, adoption of cyber insurance products remains limited due to lack of trust, inadequate understanding of policy coverage and concerns regarding claim settlement. Customer trust therefore becomes a critical factor in determining the success of cyber insurance products in India.

### **2. Objectives of the Study**

- To examine the level of awareness regarding cyber insurance products in India.
- To identify factors influencing customer trust in cyber insurance providers.
- To analyse determinants affecting the adoption of cyber insurance products.
- To provide recommendations for improving customer confidence and adoption rates.

### **3. Research Questions**

- What factors influence customer trust in cyber insurance products?
- How does awareness affect adoption decisions?
- What barriers discourage customers from purchasing cyber insurance?
- What measures can insurers adopt to improve customer confidence?

### **4. Review of Literature**

Existing studies indicate that cyber insurance is becoming an important component of enterprise risk management. Research suggests that customers are more willing to purchase cyber insurance when insurers provide transparent coverage, efficient claims processing and reliable customer

support. Research in India also indicates that awareness regarding cyber insurance among retail consumers remains relatively low when compared to health and life insurance products. This creates an opportunity for insurers to improve education and outreach initiatives.

P8: Regulatory support and credible industry standards contribute to customer confidence in cyber insurance.

P7: Digital literacy strengthens customers' ability to understand and evaluate cyber insurance products.

P6: Perceived affordability of premiums positively influences cyber insurance adoption.

P5: Better perceived service quality strengthens customer trust and adoption intention.

P4: Greater transparency in policy terms and claim procedures strengthens customer trust.

P3: Higher customer trust in the insurer is positively associated with cyber insurance adoption intention.

P2: Higher perceived exposure to cyber threats is positively associated with the intention to purchase cyber insurance.

P1: Greater awareness of cyber risks is positively associated with customer intention to adopt cyber insurance.

Based on the above theoretical discussion, the study may be guided by the following propositions:

### **5.7 Theoretical Propositions**

The proposed conceptual relationship can be represented as follows: Cyber Risk Awareness + Perceived Cyber Risk + Digital Literacy → Evaluation of Cyber Insurance → Trust in Insurer (reliability, transparency, competence, fairness and data confidentiality) → Adoption Intention. Pricing, service quality and regulatory support act as important contextual factors influencing the strength of these relationships.

Customer trust can therefore be positioned as a key intervening construct between the characteristics of the insurance provider and the customer's adoption decision. In conceptual terms, stronger awareness and perceived cyber risk may increase the need for protection; trustworthy insurer characteristics and good service quality can convert that need into confidence; and confidence, together with affordability and perceived usefulness, can lead to adoption intention.

The theoretical arguments suggest an integrated relationship among awareness, perceived cyber risk, insurer reputation, service quality, pricing, regulatory support, digital literacy, customer trust and adoption intention. Awareness and digital literacy help customers understand cyber threats and available insurance solutions. Perceived cyber risk creates the motivation to seek protection. Insurer reputation, service quality, transparency and regulatory support shape customer trust, while pricing and affordability influence the perceived feasibility of adoption.

### **5.6 Integrated Conceptual Framework**

For cyber insurance, service quality extends beyond conventional insurance administration. Customers may require technical assistance, incident response coordination, data recovery support and guidance on regulatory or legal obligations. Therefore, insurers that integrate insurance protection with cyber security expertise may create stronger perceived value and trust.

Service quality is also theoretically important because insurance is an intangible service in which the value of the product is often experienced most clearly when a claim or cyber incident occurs. In this context, responsiveness, reliability, assurance, transparency and customer support can influence customer evaluations of the insurer. Efficient communication during underwriting and

claims, knowledgeable support personnel and timely incident response can strengthen confidence in the provider.

### **5.5 Service Quality and Customer Trust**

Applied to cyber insurance, customers first assess the severity of cyber threats such as ransomware, identity theft, data breaches and financial fraud. They then assess whether cyber insurance is an effective response, whether the premium is affordable and whether the insurer can provide support when an incident occurs. Consequently, perceived severity and vulnerability may create the need for protection, while perceived effectiveness, affordability and trust determine whether that need is translated into purchase intention.

Protection Motivation Theory (PMT) helps explain how individuals respond to threats and decide whether to adopt protective measures. The theory emphasizes two broad appraisal processes: threat appraisal and coping appraisal. Threat appraisal involves assessing the severity and likelihood of a threat, while coping appraisal concerns whether the recommended protective action is effective, feasible and within the individual's ability to undertake.

### **5.4 Protection Motivation Theory**

A higher perception of cyber exposure can increase the motivation to obtain protection; however, high uncertainty about coverage may have the opposite effect. For example, if customers believe that policy exclusions are difficult to understand or that claims may be rejected, they may perceive the insurance product as risky despite being aware of cyber threats. This indicates that insurers must reduce both cyber risk perceptions and product-related uncertainty through clear communication and transparent coverage.

Perceived risk theory explains why customers may hesitate to purchase a product when the outcome is uncertain. Cyber insurance involves several forms of perceived risk, including financial risk, privacy risk, performance risk, legal or contractual risk and uncertainty regarding claim settlement. Customers may therefore evaluate not only the risk of suffering a cyber incident but also the perceived risk associated with purchasing the insurance itself.

### **5.3 Perceived Risk Theory**

Perceived usefulness represents the extent to which customers believe that cyber insurance can provide meaningful financial and risk-management benefits. Perceived ease of use reflects how easily customers can understand product information and complete insurance-related activities through digital channels. When customers perceive the product and its digital service process as useful and easy to understand, their intention to adopt may increase. Thus, digital accessibility can complement trust and awareness in explaining adoption behaviour.

The Technology Acceptance Model (TAM) provides another useful perspective for understanding adoption. Although cyber insurance is a financial protection product rather than a technology product itself, its purchase and servicing increasingly take place through digital platforms. Customers may evaluate the usefulness and ease of using online insurance services, including digital quotation, policy purchase, risk assessment, claim registration and claim tracking.

### **5.2 Technology Acceptance Perspective**

Accordingly, customer trust is expected to influence both purchase intention and willingness to continue using cyber insurance services. Transparent policy wording, fair claim settlement, protection of customer data and effective incident support can strengthen trust, while ambiguous exclusions, delayed claims and inadequate communication can weaken it.

Trust in cyber insurance can be understood through three closely related attributes: ability, benevolence and integrity. Ability refers to the insurer's technical and professional competence in assessing cyber risks and managing claims. Benevolence reflects the perception that the insurer will act in the customer's interest during a cyber incident. Integrity refers to consistency, honesty, transparency and adherence to clearly communicated policy conditions. These dimensions are particularly relevant because cyber insurance involves technical risks that customers may not be able to evaluate independently.

Trust theory provides a central theoretical basis for understanding customer confidence in cyber insurance. Trust can be viewed as the willingness of one party to depend on another when the outcome involves uncertainty and vulnerability. In the context of cyber insurance, customers face uncertainty about the occurrence of cyber incidents, the extent of financial loss, policy interpretation and the insurer's response during claim settlement. Therefore, customers are more likely to consider purchasing a cyber insurance product when they perceive the insurer as trustworthy.

### **5.1 Trust Theory**

The theoretical foundation of this study is based on the view that adoption of cyber insurance is not determined by cyber risk alone. Customers must also believe that the insurer is competent, reliable, transparent and capable of providing meaningful protection when a cyber incident occurs. The existing paper identifies awareness, perceived cyber risk, insurer reputation, pricing, service quality, regulatory support and digital literacy as important determinants of adoption. These determinants can be explained more systematically through established theories of trust, technology adoption, perceived risk and protection motivation.

## **5. Theoretical Foundation and Conceptual Framework**

### **6. Cyber Insurance in India**

Cyber insurance is a specialized form of insurance designed to protect individuals and organizations against financial losses arising from cyber incidents such as data breaches, ransomware, phishing, cyber extortion, identity theft, business interruption and third-party liabilities.

India's rapid growth in UPI, digital banking, e-commerce, cloud computing, fintech and remote working has increased dependence on digital systems and consequently increased exposure to cyber risks. Your paper similarly identifies cyber insurance as an important financial protection mechanism, while highlighting that customer trust and awareness remain important barriers to adoption.

### **7. Customer Trust in Cyber Insurance**

Customer trust is a critical factor influencing the acceptance and adoption of cyber insurance products. Unlike traditional insurance products, cyber insurance involves risks that are complex, evolving and difficult for customers to evaluate. Customers may not fully understand the nature of cyber threats, policy exclusions, coverage limitations or the process involved in making a cyber-insurance claim. Therefore, confidence in the insurer becomes an important determinant of purchase intention.

In the context of cyber insurance, customer trust refers to the customer's belief that the insurance provider is competent, reliable, transparent and capable of fulfilling its commitments when a cyber

incident occurs. A customer who trusts an insurer is more likely to believe that the insurer will provide appropriate protection, handle sensitive information responsibly and settle legitimate claims fairly.

The existing paper identifies five important dimensions of customer trust: reliability, transparency, fairness in claim settlement, data privacy and confidentiality, and competence in handling cyber incidents.

### **8. Determinants of Adoption**

**Awareness:** Customers who understand cyber risks are more likely to purchase cyber insurance.

**Individuals and businesses experiencing higher exposure to cyber threats show greater willingness to adopt cyber insurance**

**Insurer Reputation:** Strong brand image and credibility increase customer confidence.

**Pricing and Affordability:** Premium affordability significantly influences adoption decisions.

**Service Quality:** Responsive customer service and efficient claims processing strengthen trust.

**Regulatory Support:** Government initiatives and IRDAI guidelines encourage market development.

**Digital Literacy:** Customers with higher digital literacy are more willing to consider cyber insurance products.

### **9. Challenges**

- Complexity of policy wording.
- Difficulty in estimating cyber risks.
- Rapidly changing threat environment.
- Lack of historical data for pricing.
- Fear of claim rejection.
- Shortage of cyber risk specialists

### **10. Opportunities**

India's rapid digital transformation provides significant opportunities for cyber insurance growth. Expansion of fintech, e-commerce, digital healthcare and smart manufacturing will increase demand for cyber risk protection. Artificial intelligence and big data analytics can improve underwriting and fraud detection, thereby improving customer confidence.

### **11. Recommendations**

1. Conduct nationwide awareness campaigns on cyber risks.
2. Simplify policy documents and improve transparency.
3. Introduce affordable cyber insurance products for individuals and SMEs.
4. Improve claims settlement efficiency through digital platforms.
5. Strengthen partnerships between insurers and cyber security firms.
6. Encourage regulatory frameworks supporting cyber risk management.
7. Use AI and analytics for personalized risk assessment and pricing.

### **12. Implications for Industry**

Insurers should view cyber insurance not merely as a product but as a comprehensive risk management solution. Combining prevention services, incident response support and financial protection can improve customer trust and long-term retention.

### **13. Conclusion**

Cyber threats are expected to increase as India advances towards a digital economy. Cyber insurance can play a significant role in protecting individuals and businesses from financial losses

arising from cyber incidents. Customer trust remains the foundation for successful adoption of cyber insurance products. Insurers that focus on transparency, service quality and customer education will be better positioned to expand the cyber insurance market in India.

### **References**

1. IRDAI Annual Reports.
2. OECD (2024). Cyber Insurance and Risk Management.
3. Swiss Re Institute Reports on Cyber Risk.
4. World Economic Forum Global Risks Report.
5. McKinsey & Company Reports on Digital Insurance.
6. Deloitte Insights on Cyber Insurance Market Trends.
7. PwC Global Digital Trust Insights Report.
8. NASSCOM Cybersecurity Reports.
9. Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451–474.
10. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93–114.
11. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
12. Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734.