Analysis of Cyber Risk Challenges and Insurance Mechanisms

Luojia Ping

China Economics And Management Academy, Central University of Finance and Economics, Beijing 100081, China
anyu75477@gmail.com

Abstract. As the pace of digitalization accelerates, cyber risks such as data breaches, ransomware, and system outages have become significant threats to businesses and society. However, traditional insurance mechanisms provide inadequate coverage against these risks, making cyber insurance an emerging tool for risk management. This paper systematically summarizes the definitions, characteristics, and classifications of cyber risks and insurance based on a review of relevant literature and focuses on exploring the core pathways through which insurance mechanisms address cyber risks, namely risk transfer, risk prevention and control, and industry collaboration. The study points out that the current insurance market faces multiple obstacles. On the one hand, product design and risk suitability are inadequate, making it difficult to cover emerging risks, and ambiguous exclusion clauses lead to claims disputes. Additionally, industry operational mechanisms are constrained, with insufficient actuarial data and information asymmetry exacerbating pricing challenges and adverse selection. Finally, external environmental constraints are significant, with insufficient risk awareness among enterprises leading to low insurance uptake, and cross-border data sovereignty conflicts impacting claims execution. This study aims to provide references for the insurance industry and policymakers to promote the insurance market's role in safeguarding cybersecurity.

Keywords: Cyber Risk, Cyber Insurance, Risk Transfer.

1 Introduction

With the rapid development of the digital economy, cyber risks have become a significant threat to business operations. Frequent incidents such as data breaches and ransomware attacks have caused substantial economic losses and reputational risks for businesses and public institutions. Traditional insurance primarily covers natural disasters or property damage, offering limited coverage for such new risks, leaving businesses without effective risk mitigation strategies when facing cyber-attacks. Against this backdrop, cyber insurance has emerged as an important tool for addressing cyber threats. It not only provides financial compensation but also contributes to improving businesses' cybersecurity levels through underwriting, risk assessment, and the establishment of security standards. Therefore, conducting a systematic review of the current

A. J. Moshayedi (ed.), *Proceedings of the 2025 International Conference on Hybrid Commerce, Human Capital, and Economic Dynamics (ICHCH 2025)*, Advances in Economics, Business and Management Research 374,
https://doi.org/10.2991/978-2-38476-585-0_83

state, characteristics, and issues related to cyber risks and cyber insurance holds important theoretical and practical significance.

This paper adopts a literature review method to systematically organize representative studies on cyber risks and insurance both domestically and internationally. By summarizing existing academic literature, it identifies core viewpoints in the research field and analyzes the definitions, characteristics, classifications, existing issues, and recommendations for cyber risks and insurance from various perspectives. The research objectives and significance of this paper lie in providing theoretical support and practical references for the further development of cyber insurance through a systematic review of existing research findings. It helps the academic community clarify the research trajectory of cyber risk and insurance, identify research gaps, and propose new research topics. It also provides decision-making references for regulators, promoting the insurance market to better support cybersecurity.

2 Definition, Characteristics, and Classification of Cyber Risks and Insurance

2.1 Definition, Characteristics, and Classification of Network Risks

Cyber risk generally refers to the losses and risks that may arise when businesses and individuals use information systems and computer networks. Academics have provided different definitions of cyber risk from technical, economic, and legal compliance perspectives. From a technical perspective, relevant scholars believe that network risk belongs to operational risk and is related to digital events [1]. These incidents include theft, compromise, or destruction of information and/or technical assets, as well as internal and external fraud and business disruptions [1]. From an economic perspective, relevant scholars believe that cyber risk is related to malicious electronic events [2]. From a legal compliance perspective, the Bank for International Settlements (BIS) and International Organization of Securities Commissions (IOSCO) believe that cyber risk is related to the likelihood of incidents and their potential consequences [3]. Compared to traditional risks, scholars have summarized the following five characteristics of cyber risk. Cyber risk is constantly evolving and difficult to model. Cyber risk events are highly interconnected, as computer technology and infrastructure are universal, meaning that cyber risk in any location can impact the global landscape. Cyber risk can result in significant losses. Cyber risk exhibits heterogeneity. The consequences of cyber risk are largely dependent on the attacker's objectives [4].

Related research classifies the main types of cyber risks using two criteria: the source of the risk, i.e., whether it originates from within or outside the organization, and the mindset associated with the risk, i.e., whether it is caused by malicious intent. Using this approach, cyber risks can be divided into four categories. Internal malicious risks stem from unauthorized actions by internal personnel (employees or contractors), such as theft, destruction, encryption, or tampering with corporate data, or cyber extortion. External malicious risks stem from unauthorized actions by external actors (such as nations, criminals, hacker activists, or individuals), including commercial espionage,

denial-of-service attacks (DoS/DDoS), and so on. Internal non-malicious risks, which result from accidental exposure of sensitive data due to system configuration errors, human operational mistakes, or negligence within the organization. Examples include system misconfigurations that expose confidential data, or employees accidentally transmitting or losing data. External non-malicious risks, which stem from external events or environmental factors causing data exposure, such as vulnerabilities in third-party systems, operational errors by outsourcing partners, or accidental disclosure of sensitive information on public platforms, leading to unauthorized access, theft, or leakage of corporate data [5].

2.2 Definition, Characteristics, and Classification of Cyber Insurance

Cyber insurance, in simple terms, is a financial tool that businesses use to address cyber risks. Through an insurance contract, potential losses resulting from cyber incidents are transferred to the insurance company. Scholars view cyber insurance as a supplementary mechanism aimed at further reducing the financial impact of cyber-attacks, even when attackers have already penetrated the system, provided that the system has already implemented defensive measures and resilience mechanisms to maintain system-level operations [6]. Generally speaking, the phased process of cyber insurance involves the assessor first evaluating the parameters related to the risk subject. Next, the assessor will integrate the aforementioned parameters and consider the likelihood of the event occurring and its potential impact. Subsequently, the insured and the insurer will negotiate and agree on the scope of the contract and its price. Finally, if a contract has been signed and an accident occurs between the insurer and the insured within the period specified in the contract, the insured has the right to file a claim with the insurance company to compensate for property and other losses incurred [7]. Scholars have pointed out that cyber insurance has two major advantages [8]. Insurance coverage assigns a price to cyber risks, thereby incentivizing appropriate risk behavior. At the same time, companies can recognize the threat of risk by applying for cyber insurance, thereby protecting themselves. However, cyber insurance also has some drawbacks. First, the losses incurred are random, meaning that risk aggregation cannot be effectively carried out, the risk pool is too small, and diversification is difficult to achieve. Information asymmetry also hinders insurance due to moral hazard and adverse selection phenomena. Additionally, insurance coverage is often incomplete, such as policies having maximum limits, exclusions in policies, indirect costs being unmeasurable and typically not covered, and potential issues with product complexity [8].

Regarding the classification of cyber insurance, relevant scholars believe that insurance companies have developed two different types of cyber insurance, namely first-party insurance and third-party insurance, to serve companies in the IT industry and other industries in terms of cybersecurity. First-party insurance covers digital asset damage and cyber extortion, among other things. Third-party insurance covers security and privacy breaches and third-party contractual liability, among other things [7].

3 Core Pathways for Insurance Mechanisms to Address Cyber Risks

3.1 Risk Transfer

Basic network insurance provides coverage for data restoration, direct costs of business interruption, and other risks, offering SMEs the lowest level of risk transfer and meeting their basic needs. Relevant scholars have pointed out that cybersecurity insurance covers security incidents such as external network attacks and cybersecurity vulnerabilities and is an insurance product with functions such as risk dispersion and loss transfer. Developing a risk quantification assessment system can help improve the scientific nature of insurance rates, reduce risk exposure, and improve historical risk databases [9]. Unlike a single compensation mechanism, cybersecurity insurance is a comprehensive solution that integrates risk management and risk transfer. Relevant scholars have proposed that the new cybersecurity insurance product ecosystem differs from traditional cybersecurity insurance, driven by a six-step approach that includes pre-insurance diagnosis, pre-insurance treatment, in-insurance services, in-insurance monitoring, post-insurance rescue, and post-insurance compensation, primarily reflecting the principle of risk reduction [10]. Small and micro-enterprise inclusive cybersecurity insurance adopts an "insurance + service" model, while large and medium-sized industry demonstration cybersecurity insurance adopts an "insurance + dynamic monitoring + service" model. These models provide enterprises with third-party comprehensive security dynamic monitoring and evaluation optimization, reduce cybersecurity compliance costs and legal liabilities, offer high compensation limits, and provide precise security repair services [10].

3.2 Risk Prevention and Control

Insurance companies often conduct pre-underwriting risk assessments, collaborating with security vendors to provide vulnerability scanning and asset assessments for businesses, systematically evaluating the vulnerabilities of critical infrastructure, and implementing differentiated pricing based on risk levels to establish tailored coverage scope. Relevant scholars have proposed insurance schemes designed based on power system reliability and network vulnerability, combining network intrusion modeling and reliability impact to estimate premiums, with the assessment and pricing results incentivizing higher defensive investments [11]. In addition to pre-assessment, cyber risk prevention also includes dynamic risk monitoring during underwriting. Practical approaches often leverage emerging technologies for real-time data collection and status monitoring, such as blockchain-based integrated IoT platforms that generate comprehensive and tamper-proof logs and allow device owners to easily access devices deployed across different domains [12]. Through this approach, the platform enhances data access capabilities and ensures the integrity of sensor data.

3.3 Industry Collaboration

In many high-risk industries, a single company or insurance provider may struggle to handle the losses from extreme cyberattacks on their own, so cross-industry cooperation or mutual insurance pools are super important. Related scholars have proposed establishing a mutual insurance model, which can be implemented by third-party insurers or mutual insurance platforms to use financial means to hedge the individualized risks faced by transmission operators due to cyberattacks [13]. This model achieves industry-wide collaborative risk management through risk diversification, thereby enhancing the feasibility and effectiveness of cybersecurity investments.

4 Existing Issues and Recommendations for Insurance Mechanisms to Address Cyber Risks

4.1 Inadequate Product Design and Risk Suitability

The current scope of coverage for cyber insurance products lags behind the evolution of risks, failing to effectively address threats such as AI-generated content infringement, metaverse asset theft, and warfare. Scholars have focused on the period of the Russia-Ukraine conflict, studying the causal relationship between war exclusions and the scope of corporate cyber insurance coverage during this time. They found that insurance companies often narrow the scope of coverage by avoiding clear and explicit language, and these terms actually fail to provide comprehensive coverage for hybrid warfare and cyber warfare. To effectively mitigate and suppress cyber risks, insurance providers should ensure transparent implementation of comprehensive coverage and supplement it with risk prevention mechanisms [14]. By establishing well-defined cyber insurance policies to redistribute risks within the internet, market forces can help establish an order that remains difficult for state power and legal provisions to fully regulate.

Exclusion clauses in cyber insurance policies are generally vague. Scholars have studied German market insurance regulations and pointed out that the ambiguity in wording regarding explicit and implicit coverage of cyber risks poses significant risks to insurance companies [15]. Current clauses should redefine risks and expand their definitions, thereby enabling policyholders to better understand the scope of liability while also facilitating regulatory actions.

4.2 Obstacles to Industry Operation Mechanisms

One of the obstacles to current online insurance pricing is the need for more actuarial data [16]. Existing premiums often do not reflect reasonable loss estimates, but are set at higher levels to retain profits, or come with excessive disclaimers that undermine the value of insurance. Based on this, a simplified framework for premium calculation using nine factor weights has been proposed. The pricing accuracy of this model is comparable to SERFF, but the operational burden is significantly reduced. The simplified pricing method makes online insurance more practical as a risk mitigation tool.

Information asymmetry is also an obstacle to the development of cyber insurance, as companies often conceal their cybersecurity investments, making it difficult for insurers to accurately assess risks, leading to high premiums and inadequate coverage. If the insurer is unable to effectively monitor the implementation of cybersecurity measures by the insured company, issues such as information asymmetry, loss correlation, and security interdependence can hinder the effective implementation of cybersecurity risk management. As a result, the CRISM tool was developed, which can be used to score cybersecurity risks while also mitigating them [17]. The tool estimates the probability of cyberattacks by monitoring and scoring cyber risks, generates risk scores by combining asset value and vulnerability information, helps businesses optimize their defense strategies, and has the potential to reduce insurance premiums.

4.3 External Environmental Constraints

Companies lack awareness of the importance of investing in cybersecurity. Many companies rely on free security tools and are not sufficiently alert to the dangers of cyber risks, resulting in a lack of willingness to purchase insurance. Relevant scholars believe that companies and individuals have systematic cognitive biases, often underestimating cyber risks, which hinders effective risk management. Therefore, courts should recognize the legal obligation to protect data. This obligation is not only reflected in economic losses, but also in the damage to privacy and autonomy [18].

5 Conclusion

This paper uses a literature review method to systematically organize cyber risks and insurance. From the perspectives of definition, characteristics, and classification, this paper elucidates the fundamental concepts of cyber risks and insurance. Through a synthesis of relevant academic research, this paper further summarizes three approaches that insurance mechanisms employ to address cyber risks: risk transfer, risk prevention and control, and industry collaboration. Among these, risk transfer embodies the basic function of insurance, which is to mitigate direct losses caused by cyber incidents through a claims settlement mechanism. Risk prevention emphasizes the incentive role of insurance products in encouraging enterprises to increase their investment in information security. Industry collaboration highlights the significant role of insurance in promoting cross-departmental information sharing and security construction.

Further analysis indicates that the development of cyber insurance currently faces multiple obstacles. Insufficient product design and risk adaptability, ambiguous exclusion clauses, and coverage scope lagging behind risk evolution have led to persistent coverage gaps. Industry operational mechanisms are constrained, with insufficient actuarial data leading to unreasonable pricing, and information asymmetry exacerbating adverse selection and moral hazard issues. External environmental constraints are significant, with insufficient risk awareness among enterprises, cross-border data sovereignty, and regulatory differences all posing challenges to the implementation of insurance claims. Therefore, efforts should be made to promote transparency in cyber insur-

ance terms and conditions to reduce claims disputes and enhance market trust. Additionally, data sharing and risk modeling capabilities should be strengthened to establish a more robust actuarial foundation. Finally, cross-border legal and regulatory coordination should be promoted to facilitate international cooperation mechanisms on issues such as data sovereignty and claims jurisdiction.

The pace of evolution in cyber risks will continue to accelerate, and the insurance industry should further integrate technologies such as artificial intelligence and scenario simulation to enhance risk identification and pricing capabilities. Additionally, cyber insurance should transition from a single compensation tool to a comprehensive risk management mechanism. Through collaboration with governments, technology companies, and industry associations, a more robust cybersecurity ecosystem should be established to facilitate the important role of insurance in safeguarding economic and social stability in the digital age.

References

1. Curti F, Gerlach J, Kazinnik S, Lee M, Mihov A: Cyber risk definition and classification for financial risk management. Journal of Operational Risk (2023)
2. Mukhopadhyay A, Chatterjee S, Saha D, Mahanti A, Sadhukhan S: Cyber-risk decision models: To insure IT or not? Decision Support Systems **56**, 11–26 (2013)
3. Committee on Payments and Market Infrastructures & Board of the International Organization of Securities Commissions: Guidance on cyber resilience for financial market infrastructures. Bank for International Settlements and International Organization of Securities Commissions (2016)
4. Chen H, Shi Z Y: Research on Cyber Risk and Insurance: A Literature Review and Research Outlook. Wuhan Finance (05), 66–74 (2022)
5. Scheuermann J E: Cyber risks, systemic risks, and cyber insurance. Penn State Law Review **122**(3) (2018)
6. Liu S, Zhu Q: Cyber Insurance for Cyber Resilience. ArXiv abs/2312.02921 (2023)
7. Marotta A, Martinelli F, Nanni S, Orlando A, Yautsiukhin A: Cyber-insurance survey. Computer Science Review **24**, 35–61 (2017)
8. Biener C, Eling M, Wirfs J: Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance - Issues and Practice **40**, 131–158 (2014)
9. Zhang Z Y, Sun Y W, Sun Q W: How to Quantitatively Assess Risks in Cybersecurity Insurance. Confidentiality Work (01), 51–53 (2024)
10. Zhou J H: Cybersecurity insurance helps improve cybersecurity risk management. China Information Security (10), 41–43 (2023)
11. Lau P, Wang L, Liu Z, Wei W, Ten C W: A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability. IEEE Transactions on Power Systems **36**(6), 5512–5524 (2021)
12. Hang L, Kim D H: Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. Sensors **19**(10), 2228 (2019)
13. Lau P: An Insurance Framework for Cyber-Physical Power Systems Considering Integrated Cybersecurity-Reliability Assessment. Doctoral dissertation (2021)
14. Cremer F, Sheehan B, Mullins M, Fortmann M, Ryan B J, Materne S: On the insurability of cyber warfare: An investigation into the German cyber insurance market. Computers & Security **142**, 103886 (2024)

15. Wrede D, Stegen T, Graf von der Schulenburg J M: Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. Geneva Papers on Risk and Insurance Issues and Practice **45**, 657–689 (2020)
16. Snavely D: Rapid Estimation for Cyber Insurance Premium Pricing for Company Decision-Makers. Doctoral dissertation (2023)
17. Shetty S, McShane M, Zhang L, Kesan J P, Kamhoua C A, Kwiat K, Njilla L L: Reducing Informational Disadvantages to Improve Cyber Risk Management. Geneva Papers on Risk and Insurance **43**(2), 224–238 (2018)
18. Kesan J P, Hayes C M: Liability for Data Injuries. University of Illinois Law Review **2019**(1), 295–363 (2019)