WEP Warwick Evans Publishing

International Journal of Global Economics and Management

ISSN: 3005-9690 (Print), ISSN: 3005-8090 (Online) | Volume 5, Number 2, Year 2024
DOI: https://doi.org/10.62051/ijgem.v5n2.15
Journal homepage: https://wepub.org/index.php/IJGEM/index

Exploring the Way to Improvemnet in the Cyber Insurance Industry

Jinxuan Cai *

Law School, Shenzhen University, Shenzhen, 518000, Guangdong, China
*Corresponding Author: 18319776833@163.com

ABSTRACT

Cyber insurance is a nascent form of insurance in the digital economy. Its potential for growth and integration within industrial ecosystems in China has garnered increasing interest from academic circles in recent years. China stands to benefit from the promising prospects of cyber insurance, bolstered by national policy support and a dual focus on stimulating both supply and demand. The operational mechanism for establishing uniform norms remains imperfect, and there is a need to clarify the legal attributes of cyber insurance, its operational mechanism, and the types of insurance, as well as to address the unique challenges and issues of cyber insurance from the perspective of the insured to the insured. This paper analyses the characteristics and deficiencies of the primary development stage of China's existing cyber insurance industry based on existing research at home and abroad. It also puts forward suggestions for the improvement of China's cyber insurance industry from the perspective of the internal participant in the cyber insurance industry.

KEYWORDS

Cyber insurance; Insurance law; Cybersecurity law; Silence cyber exposure; Moral hazard; Adverse selection

1. INTRODUCTION

Cyber insurance is used to protect businesses and individuals from Internet-based risk. Companies that use a computer, receive, transmit electronic data, store information, or connect to the Internet are exposed to cyber liability. [1] Cyber insurance is an unavoidable way to avoid risks in the operation of enterprises and the provision of digital products and services in the era of digital economy, and it is an emerging type of insurance that provides insurance protection for network security risks, which has increasingly become an important tool for dispersing and preventing network security risks, and plays an important role in promoting the construction of network security socialized service system. Its emergence and development in common law countries is earlier than that in China, and its mode of operation has already had a certain scale.

Most of the domestic research on cyber insurance starts from the perspective of the government and insurance enterprises, and scholars refer to the experience of the more mature cyber insurance industry in the West, such as in Drawing on the Development Experience of cyber insurance in the United States. [2] written by Ma Da, summarized the experience of U.S. cyber insurance in terms of sound laws and regulations, government-led, cross-institutional cooperation to optimize cybersecurity services, and various types of enterprises playing the main advantages. Jiang Yan and Chen Yufan, in their article "Opportunities for cyber insurance Development in China from the Global Development History"[3], also summarized the development experience of cyber insurance in the United States and Europe, which is presented from the perspectives of promotion of laws and

regulations, guidance of professional organizations, and independent exploration of industrial subjects; the above summaries provide Chinese scholars with a concise introduction for their preliminary understanding of cyber insurance, and are also in line with the characteristics of the uneven development of cyber insurance worldwide.

Scholars also summarized the promotion of cyber insurance and the market potential for the development of cyber insurance in China. In response to the existing problems of cyber insurance in China, Lv Xiuping and Tian Bingxin, in their "Strategy for the Promotion of cyber insurance in China [4] in which they summarized the current situation of cyber insurance popularization: low participation rate, limited consumer understanding, and insufficient product supply. In Zhang RuChao's article "Exploration and Reflections on the Development Path of cyber insurance"[5], He put forward three specific problems regarding the problems of cyber insurance in China: incompleteness of industry standards, incomplete product system, and lack of social cognition; the above scholars' summaries have been objective analyses of the current situation of the development of cyber insurance in China. Some scholars analyzed the legal attributes of cyber insurance, the necessity of participating in cybersecurity governance and institutional obstacles from the perspective of services provided by cyber insurance, for example, in the article "Institutional Dilemmas and Relief Ways of Insurance Participation in Cybersecurity Governance in the Era of Digital Economy"by Zhou Ruiyu and Zhao Jingwu, [6] according to cyber insurance applied to network security governance system necessity and system obstacles, they combine cyber insurance and cyber security legislation to analyze where cyber security insurance is going, which is instructive to the authors.The academic research of the above scholars is in line with the basic situation of China's network security insurance in the initial stage. This paper will further elaborate specific problems of cyber insurance itself, and the shortcomings of different existing insurance products in protecting the property loss and liability suffered by enterprises in cybersecurity risks; and provide suggestions for further promoting the development of cyber insurance industry.

2. CHARACTERISTICS OF CHINA'S EXISTING CYBER INSURANCE SYSTEM

2.1. Decentralizing the Silence Cyber Exposure

Cyber insurance, as an emerging type of insurance, combines the functions of cyber risk management and claims settlement for economic losses. In the era of digital economy, enterprises will encounter data leakage, business interruption and other cybersecurity threats other than traditional risks in their operations. In the context of insurance, the term "silent cyber exposure" refers to cybersecurity risks that are not explicitly excluded from property all-risks and other liability insurance policies. [7] The reason for the emergence of silent cyber exposure is that before the emergence of cyber insurance, cyber risks, as risks not explicitly included in the terms and conditions of the insurance contract, could only be covered by accidental loss insurance, business interruption insurance and other traditional types of insurance. However, based on the complexity and variability of the causes of cybersecurity accidents, and with the economic losses caused by cyber risks rising year after year, the insurance industry has split the types of insurance covering cyber risks to independently underwrite property losses. Compared to cyber risks that may arise under traditional insurance contracts as to whether or not the insurance company is responsible for compensation, clear contractual terms and specific cybersecurity risk assessment of cyber insurance can determine the scope of coverage of cyber insurance contracts, reducing the risk of additional liability for the insurance company while reducing the risk of additional liability to pay claims, and allowing companies to manage cyber risks as well as enter into the claims stage through clear contractual terms Improve the efficiency of risk management, so that the demand for insurance can be fully satisfied.

2.2. Provision of Limited Cyber Risk Loss Cover for Businesses

In light of the numerous cyber incidents that have occurred in practice, insurance companies are primarily responsible for settling claims in the following instances: business interruption resulting from cyber infringement which leading to economic losses; economic losses due to data loss and inaccessibility caused by cyber ransom attacks; and repair costs associated with restoring information systems and data. Additionally, insurance companies are liable for damages incurred due to third-party economic interests, personal data leakage, or data leakage of upstream and downstream enterprises resulting from cyber infringement. [8] In the event that an insured enterprise suffers a cyber incident, in addition to guaranteeing the direct economic loss of the insured enterprise, the cyber insurance will fill in the loss for the tort damages liability borne by the insured enterprise and the insured due to the cyber incident, instead of filling in all the losses of the third party caused by the cyber incident. China's Tort Liability Law, based on the purpose of protecting the rights of victims, expands the scope of liable persons by providing that the person ultimately liable for compensation shall bear the ultimate liability for compensation, which is not true joint and several liability. However, the expansion of the scope of the responsible person is prone to make the scope of the main responsibility of network service providers fall into an ambiguous dilemma. Therefore, from the perspective of protecting the interests of network service providers, network security insurance is a self-remedial means for the insured enterprises of network service providers to get losses filled in the wake of assuming the untrue joint and several liabilities in the event of network infringement behavior.

3. CURRENT SHORTCOMINGS OF THE CYBER INSURANCE SYSTEM

3.1. Adverse Selection and Moral Hazard Caused by Information Asymmetry

In the context of cybersecurity risks, policyholders, insureds and beneficiaries may elect to reverse-select, that is, they may choose to forego the implementation of necessary precautions and system upgrades in instances where the likelihood of a cyber incident is high, and instead pursue the acquisition of cyber insurance, which would entitle them to receive insurance compensation. Adverse selection between the insurer and the insured can engender distrust of the insurer towards the insured, elevate the threshold for participation, and prompt the insurer to increase premiums in order to cope with the heightened level of risk incidence. Conversely, policyholders facing lower risks tend to surrender their insurance policies, and the proportion of high-risk enterprises in the total number of insured enterprises rises, which further raises the average risk and premiums and triggers disruption in the order of the insurance market.

Moral hazard arises subsequent to the signing of the insurance contract by both the insurer and the insured. It encompasses both the insured committing insurance fraud for the sake of insurance benefits and the insured adopting an indifferent attitude towards the prevention of loss or the limitation of loss due to insurance coverage. In the context of cyber insurance, the term moral hazard primarily encompasses three distinct categories of behaviour exhibited by insured enterprises. The first category pertains to instances where an enterprise deliberately creates cyber security incidents or deliberately exacerbates the extent of loss subsequent to a cyber security incident, with the objective of securing enhanced compensation for insurance premiums. This constitutes an act of insurance fraud. The second category encompasses instances where an enterprise, having taken out an insurance policy, fails to implement the requisite cyber security precautions or to maintain and update its cyber security infrastructure in a timely and effective manner. This represents an ex-ante moral hazard. The third category encompasses instances where an enterprise, having experienced a cyber security incident, fails to take proactive measures to mitigate potential losses. This represents an ex-post moral hazard. The first is the failure to implement the necessary cyber security precautions or to maintain and update the cyber security infrastructure on a regular basis after the insurance policy has been taken out, which is an ex-ante moral hazard. The second is the failure to take active measures to mitigate potential

losses after a security incident occurs, which is ex post moral hazard. The distinctive feature of moral hazard in the context of cyber insurance is the liability of the insurer for third-party damages incurred by the insured, as stipulated in the insurance product selected by the insured (liability insurance). [9] To illustrate, when a business is able to transfer its liability for consumer damage caused by cyber risks through insurance, rather than investing in cybersecurity facilities, the business will reduce its investment in security facilities due to return on investment factors. This will increase both the risk of damage to the consumer and the risk of loss to the insurer.

3.2. Limited Market Awareness and Recognition of Cyber Insurance

The limited market awareness and recognition of cyber insurance is also attributable to the fact that the insurance industry is in the exploratory phase of developing a business in this area. The majority of cyber insurance policy forms and clauses reflect the characteristics of Western policies, making it challenging for enterprises to identify an insurance product that aligns with their specific cybersecurity needs. Additionally, the lack of data on the scope of cyber insurance coverage has contributed to a lack of recognition by enterprises. The uncertain insurance coverage of cyber insurance due to the lack of data also limits the extent to which enterprises recognize the value of cyber insurance. Furthermore, the legal responsibility of enterprises to maintain cybersecurity under national legislation has yet to be perfected. China's cybersecurity legislation is confusing and conflicting in terms of the standards of punishment for illegal behavior by enterprises. Once an enterprise suffers a cybersecurity accident, it may be liable for compensation to a third party based on Article 70 of the Personal Information Protection Law [10], but there is still a lack of corresponding laws and regulations to support the identification of the liability for compensation, calculation of the compensation value, and distribution of the compensation payment. Overall, the cyber insurance market still has a large potential for development. The cyber insurance market still has considerable scope for further development. It is therefore essential that market participants and government regulators collaborate to establish insurance regulations for cyber insurance and to enhance the motivation and enthusiasm of enterprises to purchase cyber insurance products and services.

3.3. Insufficiency of Data to Inform Product Design, Pricing and Loss Determination in Cyber Insurance

The design of cyber insurance products is inextricably linked to the insurability of cybersecurity risks. It is possible to identify and price risks, which requires insurance companies to determine and quantify the probability of occurrence of risks and the expected losses caused by risks through actuarial calculations when designing insurance products. Reasonable premiums require insurance products to be designed to match the damages coverage and cybersecurity services provided, under the premise that the former must be commensurate with the latter. It is possible to identify and price risks. However, controllable losses require insurance companies to adopt co-insurance, reinsurance, and premium collection methods in order to ensure solvency when pricing risks. Furthermore, it is necessary for insurance companies to take timely emergency response measures in order to limit the expansion of losses after the occurrence of risks. In order to ensure solvency, insurance companies must adopt co-insurance, reinsurance, and premium collection in risk pricing. Furthermore, they must implement timely emergency response measures to limit the expansion of losses after the occurrence of risks. All measures to satisfy the insurability of cyber risks are inextricably linked to the analysis and calculation of historical risk data. The extant research on cyber insurance in China is predominantly qualitative in nature, employing a range of deterministic indicators to examine the underlying cyber risks. However, there is a limited focus on quantitative analysis, which could prove invaluable in addressing the challenge of cyber insurance pricing. [11] Quantitative assessment encompasses two distinct yet interrelated domains: cybersecurity risk assessment and cybersecurity capability assessment. Additionally, it incorporates a qualitative assessment of the impact of cybersecurity maturity and a quantitative assessment of the probability of cybersecurity events based

on a range of risk scenarios and inputs of diverse control measures. [12] However, the majority of risk quantification models and data actuarial models are in the possession of cybersecurity enterprises. Consequently, insurance companies are required to collaborate with these entities to complete product design and pricing, as well as loss determination. In the absence of a systematic data sharing mechanism, the design and pricing of cyber insurance products, along with loss determination, have encountered significant challenges. These obstacles must be overcome by insurance companies and their partners, as the current situation is not conducive to cyber insurance facing the challenges of the industry. In the absence of an institutional data-sharing mechanism, the obstacles and difficulties encountered in the design and pricing of cyber insurance products must be overcome by insurance companies and their partners alone. This is an impediment to the development of cyber insurance for a wider range of SMEs and to the determination of premiums and compensation limits.

3.4. Uncertainty about the Basic Coverage and Out-of-coverage Effects of Cyber Insurance

Those providing cyber insurance must accept the obligation to reimburse policyholders for the financial losses incurred as a result of cybersecurity risks. The characteristics of network security risks include their hidden nature, complexity, rapid development and scale of destruction. As cybercrime means continue to evolve, network security accidents often lack clear indications or warnings prior to the digitalisation and network enhancement stages. Furthermore, the enhanced digitalisation and networking provides a more apparent target for network attacks. The target is the operational supply chain of numerous enterprises. A network attack or improper operation resulting from network security insurance liability can have significant consequences. The supply chain operating on the "target" is linked to countless enterprises, and a cyber-attack or network security incident brought about by improper operation will often affect the normal operation of the entire supply chain, resulting in a large-scale, wide-ranging, highly correlated business interruption, data leakage and property loss. Consequently, in light of the aforementioned characteristics of cyber risks, more comprehensive coverage may even reduce the insurer's risk by diversifying the risk. Because a limited-risk insurer could be devastated if the limited risk becomes a reality because the limited-risk policy was priced entirely on an insulated risk. By contrast, a more broad-based policy that is priced accordingly has risk diversification for the insurer. [13] Furthermore, insurers will accord a high degree of importance to the inclusion of exclusion clauses and the delineation of benefit scope in policy terms, primarily from a profitability standpoint.

The exclusion clauses of cyber insurance policies designed by Chinese insurance companies provide illustrative examples. The "China Pacific Property Insurance Company Limited cyber insurance (Section A) Clauses" excludes the payment of damages caused by "mechanical failure", while the "People's Republic of China Property Insurance Company Limited Special Risks Insurance Policy for Information Security" also excludes the payment of damages caused by "any mechanical or electronic failure". The PICC Information Security Special Risks Policy similarly excludes liability for "loss or expense based on the interruption, breakdown or interruption of supply of any mechanical or electronic unit". However, this exclusion does not apply to any failure of telephones, cables or telecommunications under the direct control of the insured as a result of the insured's wrongful act or denial-of-service attack on the insured. The "Zhong An Online Property Insurance Company Limited Cyber Security Comprehensive Insurance Provisions" stipulate that the insurer shall not be responsible for indemnification in the event of an attack, invasion, illegal use or access behaviour that is not documented or a completely new pattern. This is in accordance with the chapter of exemption of liability. In the field of cyber security, the insurer is not responsible for indemnification in eighteen situations that fall outside the scope of coverage. The Zurich China Cyber Security Policy stipulates that the insurer is not liable for losses, defence costs or first party costs arising from claims or events not based on security misconduct. Security misconduct is defined as actual or alleged acts, errors, omissions, negligence or faults. or failures of duty by the insured, a person for whom the insurer is

legally liable, or a service provider causing a security incident) resulting from the sending of spam emails.

A comparative analysis of the policy terms and conditions of each insurance company revealed that the coverage provided by each insurer varies. Even for the same situation, the standard of indemnification differs. Despite Article 17 of the Insurance Law of the People's Republic of China stipulating that for the clauses exempting the insurer's liability in the insurance contract, the insurer is obliged to provide a prompt and sufficient explanation to the policyholder, either in writing or verbally, in order to draw attention to the content of the exemption clauses and to give a clear explanation of their meaning. However, an analysis of the textual explanations provided by various insurance companies reveals that the enterprises, as the insureds, do not necessarily have sufficient attention or understanding of the written descriptions of the contractual provisions. it is difficult for enterprises to know what risks an insurer may be liable to cover given continued uncertainty around the enforceability of cyber insurance exclusions and the absence of a common policy form.[14] Furthermore, it can be seen that the right to interpret the terms and conditions is largely in the hands of insurance companies. This factor is likely to become a significant consideration for enterprises when choosing insurance companies and insurance products, or even when forming a distrust of cyber insurance products. It is of great importance to clearly define the basic coverage of cyber insurance in order to ensure the sustainable development and orderly operation of the cyber insurance market.

4. WAYS TO IMPROVE THE FUNCTIONING OF THE CYBER INSURANCE SYSTEM

4.1. Improve the Supporting System of Cyber Insurance

In the absence of nationally-applicable standards for basic coverage and loss determination in China's cyber insurance market, the government is required to participate in and summarise the experience accumulated in business practice, and to form legal norms of a guiding nature. The Ministry of Industry and Information Technology (MIIT) and the State Administration of Financial Supervision (SAFS) have recently proposed a series of policies aimed at fostering the growth of cyber insurance. These policies are outlined in the Opinions on Promoting the Standardised and Healthy Development of Cyber Insurance, released by the aforementioned governmental bodies. The development of cyber insurance is contingent upon several factors, including the integration of cyber security technology, the creation of products aligned with the unique attributes of cyber security, the enhancement of standardised specifications for cyber security insurance, and the clarification of fundamental processes and common requirements pertaining to pivotal aspects such as underwriting and claims settlement. [15] Given its arbitrary nature, cyber insurance is unable to obtain independent provisions of its own separate law. The formulation of standards pertaining to the quantitative assessment of cyber risks in pivotal sectors and domains prior to underwriting, as well as the standardisation of security risk assessment criteria, represents a pivotal area of focus for government departments. Similarly, the standardisation of monitoring and early-warning methodologies, alongside the standardisation of monitoring and early-warning methods, are essential elements in this process. Furthermore, the standardisation of requirements for claims services post-underwriting, along with the standardisation of cyber insurance after-sales services, are crucial aspects that require attention. The primary focus for government departments is the establishment of supporting systems. In addition, while piloting and implementing the aforementioned policies globally, it is imperative to promote the construction of comprehensive legal norms for cybersecurity. This should include stipulating the legal responsibility for violating cybersecurity standards and norms, as well as promoting the legal obligation of controlling and preventing risks, which should be stipulated and supervised by the insurer in the insurance contract. It is essential to articulate the rules of risk governance set forth in the Insurance Law of the Peoples Republic of China and the legislation on

cybersecurity. This will ensure the legitimate interests and external social and public rights and interests of both parties to the cyber insurance contract and the insurance industry are guaranteed.

4.2. Strengthening the Regulation of Cyber Insurance Products and Their Related Businesses

China's regulatory authorities have progressively introduced more rigorous regulatory requirements for cyber insurance products and their associated businesses. These requirements pertain to product design, pricing strategies and risk assessment models, and they are intended to ensure that insurers comply with relevant standards. The State Administration of Financial Supervision and Administration has yet to issue regulatory regulations and standards focusing on cyber insurance. These would include the design requirements of cyber insurance products, the scope of coverage, the claims process, and the determination of liability and loss, among other aspects. Furthermore, the government is obliged to establish a data-sharing and flow mechanism with insurance companies and cybersecurity technology companies, and to summarise and generalise the aforementioned regulations and standards over an extended period of time. Additionally, the government is expected to collaborate with insurance companies and cybersecurity technology companies to develop a data-sharing and flow mechanism, with the aim of summarising and generalising the regulations and standards over an extended period of time.

4.3. Constructing a unified industry specification to develop and innovate cyber insurance business from the perspective of taking into account the needs of small and medium-sized enterprise market players and cross-industry cooperation

China's cyber insurance market is still in its early stages of development. In the absence of comprehensive legal frameworks, self-regulation and unified standardisation within the cyber insurance industry play a crucial role in ensuring the orderly operation and healthy development of the cyber insurance market. It is incumbent upon insurance associations to assume the role of industry coordinator. They must promote the formulation of model clauses for cyber insurance policies and norms for the fulfillment of obligations of both parties to the insurance contract. This will facilitate the participation of a greater number of insurance companies, policyholders, and insured persons in the cyber insurance market, which will be guaranteed by transparent rules. It will also stimulate market vitality and satisfy the growing cybersecurity needs of market players. It is imperative that insurance companies amass historical risk data and insurance data accumulated in the course of insurance practice. They must also reach a unified basic coverage of cyber insurance, engage in cross-field in-depth cooperation with cybersecurity technology companies in response to the development problems of pricing and loss determination, and combine with the cybersecurity products and services provided by cybersecurity technology companies to launch a program of continuous prevention of cyber risks before and during underwriting. Furthermore, they must provide insurance in accordance with the unified loss determination and compensation standards after underwriting. Insurance companies should implement a comprehensive automated cyber insurance solution of "risk management services + cyber insurance" to continuously prevent cyber insurance risks before and during underwriting, and issue insurance according to uniform loss determination and compensation standards after underwriting. Under the assumption that cyber insurance claims will be reduced in th light of stringent cyber security. Insurers will not lose out as a result of sharing part of their premium with their partner cyber security firm and thus they will not have to resort to increasing the premium.[16]In response to the diversification of cyber insurance needs, a series of customized insurance products have been launched. These products have been developed based on in-depth customer research, big data analysis and actuarial modelling. The objective is to assist policyholders and insured parties in minimizing the costs and expenditures, as well as property losses and liabilities, caused by cybersecurity risks.

5. CONCLUDING REMARKS

Cyber insurance, as a nascent form of insurance in the context of the digital economy, demonstrates considerable scope for growth and potential in China. It is recommended that the government implement stronger legislative measures and formulate supporting policies to establish a supportive framework for cyber insurance operations. This would facilitate the development of a standardised operational system and provide policy support for its implementation. It is incumbent upon insurance industry associations to formulate unified policy specifications in order to cope with evolving cyber risks and to promote insurance product innovation and market competitiveness. Concurrently, insurance companies must assume the responsibility of advancing the development of cyber insurance and create flexible and diverse insurance products to meet the security protection needs of enterprises and individuals at varying levels. Through collaborative efforts and a division of labour among the Chinese government, the insurance industry, and the insured, China's cyber insurance industry can facilitate a more robust and sustainable growth trajectory, capitalise on opportunities in the digital economy, and provide a robust guarantee for the secure operation of the digital economy.

REFERENCES

[1] Johnson, J. A. (2019/08//). 21st Century Insurance: CYBER INSURANCE. Computer and Internet Lawyer, 36(8), 15-20.

[2] Ma Da (2023). Lessons learned from the development of cyber insurance in the United States. China Insurance (11), 56-59.

[3] Jiang Yan & Chen Yufan. (2022) China's cyber insurance development opportunities from the global development history. Industrial Information Security (03), 6-12.

[4] Lv Xiuping & Tian Bingxin. (2023) Promotion strategy of network security insurance in China. Network Security Technology and Application (10), 132-133.

[5] Zheng Ruchao. (2023) Exploration and reflection on the development path of cyber security insurance. Shanghai Insurance (10), 31-34.

[6] Zhao Yaning. (2023). Institutional dilemmas and solutions for insurance participation in cybersecurity governance in the era of digital economy [J]. Insurance Research (05), 37-50. doi:10.13497/j.cnki.is.2023.05.004.

[7] Cyber insurance underwriting risk. (2016). https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2016/cp3916

[8] Zhou Rui Yu & Zhao Jingwu. (2023). Jurisprudential foundation and practical path of network security insurance . Hubei Social Science (04), 136-147. doi:10.13660/j.cnki.42-1112/c.016087.

[9] Wu Yi-wen. (2022). Reflections on Moral Risk Control Mechanism in Insurance Law [J]. Chinese and foreign law, (06), 1405-1424.

[10] Article 70 of the Personal Information Protection Law: If a processor of personal information violates the provisions of this Law by handling personal information in a manner that infringes on the rights and interests of a large number of individuals, the People's Procuratorate, a consumer organization as prescribed by law, and an organization determined by the State Internet Information Service may bring a lawsuit in the People's Court in accordance with the law.

[11] Tang Jincheng & Mo Cicong. (2022) Research on the Innovation and Development of cyber insurance in the Era of Digital Economy. Southwest Finance (01), 52-64.

[12] Fang Binxing. (2022). Enhancing the security posture of cyberspace from the perspective of "people, money and things". Proceedings of the Chinese Academy of Sciences (1), 53-59. doi:10.16418/j.issn.1000-3045.20211117006.

[13] Stempel, J. W., & Knutsen, E. S. (2018). The Techno-Neutrality Solution to Navigating Insurance Coverage for Cyber Losses. Social Science Research Network.

[14] French, C. C. (2021). Five Approaches to Insuring Cyber Risks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3811826

[15] (2023) MIIT, SFSA issue opinions to promote standardized development of cyber insurance. Information Network Security (08), 130.

[16] Soyer, B., Nicholas, A., & G. Leloudas. (2023). Cyber Risk Insurance – An Effective Risk Management Tool for SMES in the UK? Edinburgh Law Review, 27(2), 157–184. https://doi.org/10.3366/elr.2023.0826