EXPLORATION OF COMBINATION OF CYBER INSURANCE AND COMMERCIAL PROPERTY INSURANCE

A Dissertation
Submitted to
the Temple University Graduate Board

In Partial Fulfillment
of the Requirements for the Degree
DOCTOR OF SCIENCE

by
Qing Yu
Diploma Date December 2022

Examining Committee Members:

Gurdip Bakshi, Department of Finance

Xiaohui Gao Bakshi, Department of Finance

Krupa Viswanathan, Department of Risk, Actuarial Science and Legal Studies

Sudipta Basu, Department of Accounting

ABSTRACT

Along with the continuous advancement of digital transformation in various industries and fields in China, network assets and digital assets become common in the context of digital economy. In this process, increasingly frequent digital interactions have given rise to new types of cyber risks. As cyber insurance appeared late in China, most enterprise clients know little about it and thus are unlikely to accept transferring cyber risks through insurance. This results in a low take-up rate of cyber insurance. Moreover, commercial property insurance cannot meet the demand for transferring enterprise asset security risks in the context of digital economy because new-type assets, such network assets and data assets, are not covered by commercial property insurance. In light of these facts, this paper reviews the theoretical research and market expansion of cyber insurance and commercial property insurance, and discusses the feasibility of combining cyber insurance with commercial property insurance from the perspectives of market environment, legal environment, and ecosystem of cybersecurity. Then this paper expounds on the necessity of combining cyber insurance with commercial property insurance from the perspectives of market scale, objects of insurance and development of the insurance sector post COVID-19. At last, projections are made with respect to the market revenues, premiums and possible cybersecurity loss suffered by enterprises through hypothetical models and case studies to provide insights for the theoretical research and practical exploration of combination of cyber insurance and commercial property insurance in the future.

Key words: cyber insurance, commercial property insurance, cybersecurity property insurance, security threat

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Along with the continuous advancement of digital transformation in various industries and fields in China, network assets and digital assets become common in the context of digital economy. In this process, increasingly frequent digital interactions have given rise to new types of cyber risks. From the EternalBlue cybersecurity incident that broke out around the world in 2017, we know that, on the one hand, the losses caused by network damage could be very high though the security defense technology keeps evolving; on the other hand, cyber risks cannot be absolutely eliminated. Risks should be diversified or transferred to reduce losses in cyber risk management of enterprises. Based on the needs of individuals and communities as a whole, cyber insurance, which plays a key role in risk diversification, has emerged and developed rapidly in the United States and Europe since 1998. As cyber insurance appeared late in China, most enterprise clients know little about cyber insurance and thus are unlikely to accept transferring cyber risks through insurance. This results in a low take-up rate of cyber insurance. Moreover, commercial property insurance cannot meet the demand for transferring enterprise asset security risks in the context of digital economy because new-type assets, such network assets and data assets, are not covered by commercial property insurance. In this context, this paper discusses the combination of cyber insurance and commercial property insurance in terms of feasibility and necessity to provide insights for insurance institutions in insurance product innovation and insurance theory research.

2. EVOLUTION OF CYBER INSURANCE

In recent years, domestic scholars and insurance institutions have been exploring the development of cyber insurance in China in parallel with the rapid development of cyber insurance in foreign countries.

2.1 Academic Research

As an effective tool to transfer cyber risks, cyber insurance can not only safeguard the efficient operation of enterprises, but also serve as a "social stabilizer". As the academic research of cyber insurance started late in China, there have been limited academic studies found in connection with cyber insurance, mainly focusing on theoretical analysis, empirical test, legal analysis and premium setting of cyber insurance in China.

The theoretical analysis mainly deals with the basic concepts (Xu, 2022)[1], causes and drivers (Che, 2020)[2], differences between China and foreign countries (Gao, Yang, 2010; Tang and Li, 2014; Liang and Zhang, 2017)[3-5], system building (Wang, 2008; Gao and Lv, 2011)[6-7], and so on of cyber insurance from different perspectives. As for the status quo and development strategy of cyber insurance, Liu and Gao (2002)[8] analyzed the opportunities and challenges faced by the information security industry and the insurance sector in the new century and put forward certain problems and solutions in the collaboration between the information security industry and the insurance sector. Jiang (2003)[9], after introducing the status quo, analyzed the limitations of technical and legal solutions, and discussed the possible problems and countermeasures in the development of cyber insurance. Gao and Lv (2011)[7] conceived the characteristics and steps of risk management for network and information security insurance, and discussed how to promote the establishment of China's network and information security insurance system from the perspectives of policy,

regulation, law, training and education, technical cooperation, and product R&D innovation in the current context of market. Wang (2017)[10] analyzed the status quo of cyber insurance in China and other countries, analyzed the existing problems and reasons through case studies, and put forward recommendations on its development from the perspectives of legislator, regulator and insurer. Wang and Wang (2017)[11] took the life cycle of cyber insurance as a coordinated system and put forward specific recommendations for future theoretical research and practice, such as strategy, information symmetry, accurate risk determination with new technologies and methods, and strengthening of sharing of cybersecurity intelligence. Tang and Mo (2022)[12] analyzed the status quo of cyber risks and cyber insurance in the era of digital economy, and put forward policy recommendations for promoting innovation and development of cyber insurance from three aspects, i.e., insurance companies, cybersecurity enterprises and regulatory authorities.

As for empirical test, scholars often use empirical methods and models to test the externality and optimization of cyber insurance products. Gu, Mei et al. (2015)[13] studied the equilibrium results of individual optimal choice under non-cooperative game between enterprises and social optimal investment choice under cooperation between enterprises, and designed an incentive mechanism for investment in information system security for cyber insurance. Their results show that appropriate insurance deductibles can internalize the negative externality of insufficient investment in enterprises' security and improve their level of security to a certain extent. Focusing on decrease in efficiency of the cyber insurance market caused by information asymmetry, Yang and Wang (2016)[14] studied the optimal contract model for cyber insurance by taking into account of moral risks of network users, established a contract analysis model for cyber insurance by applying the principal-agent theory, and discussed its properties. Yuan (2018)[15] summed up the psychological factors

affecting risk perception through qualitative research and analysis based on a questionnaire survey, and explored the direct or indirect relationship between various factors and cyber risk perception through quantitative and empirical investigation. Dong, Xie et al. (2019, 2021)[16][17] studied the optimal decision-making on enterprise information security investment and network insurance based on the ruin probability constraint, described different types of data breach risks around the world with the Gemalto's data breach database, measured network and information security risks and corresponding premiums with optimal fitting distribution, and gave the premiums of different types of data breach under the criteria of pure premiums, expected values, and standard deviations.

Scholars from the legal community have discussed the legal and institutional issues related to cyber insurance. Wang (2011)[18] discussed the formulation of laws and policies on cyber insurance, and proposed that the laws and policies should be coordinated comprehensively and facilitated by all stakeholders. Wang (2018)[19] compared and analyzed the development of information security liability insurance in China and other countries, and explained the difficulties in constructing an information security liability insurance system from various aspects. Fang and Chu (2020)[20] reviewed the existing marine insurance risk governance system in a systematic and comprehensive manner, and put forward recommendations, such as further optimizing the specific provisions and interpretation rules of underwriting risks in China's insurance contracts based on coordination of internal and external governance rules. Zhang and Wu (2021)[21] systematically studied the building of a personal information security liability insurance system, and put forward relevant practical recommendations.

As for pricing of cyber insurance, Wang (2017)[22] constructed a multiple regression model based on the bitcoin ransomware affecting college students and studied the pricing of

insurance against bitcoin ransomware invasion. Focusing on correlation characteristics of network risks, Zhao (2019)[23] applied a hierarchical Archimedes Copula model to building correlation and investigated the pure risk premium of network and information security insurance under different correlation assumptions and different policies through scenario analysis. Chen et al. (2020)[24] determined premiums with a short-term aggregation risk model, determined four main network breach routes through principal component analysis, and established different gradient payment models for each main network breach route. Ma (2020)[25] simulated the spread of network viruses based on the SIS model of infectious disease, modeled the evolution of cyber risks with the Markov model, and studied the pricing of cyber insurance under scale-free network.

2.2 Application And Practice

In the early days, foreign property insurance companies expanded in China's cyber insurance market by leveraging their advanced experience in foreign markets and relatively mature and complete risk management systems. For example, Allianz Property Insurance, a foreign-invested insurance company in China, launched the first program of cyber insurance and reputation insurance for clients in China in 2015. In recent years, China's cyber insurance industry has gradually entered an exploratory stage from infancy with the joint efforts of all stakeholders.

As for promotion of cyber insurance, Digital World Consulting, a Chinese third-party consulting firm in the digital industry, released the *Map of Cybersecurity Capability in China (January 2020)* to categorize security capability for cyber insurance with maps for the first time, which have been gradually recognized and appreciated by the community. In October, 2021, the China Academy of Information and Communication Technology (CAICT) solicited cases of excellence from cyber insurance enterprises around the country, and selected 8 cases

of excellence after the nomination, formal review and expert review. The National Research Center for Industrial Information Security Development released typical case studies of cyber insurance in December 2021, which attracted wide attention and active participation from insurers, reinsurers, cybersecurity companies, insurance technology providers and other industrial players.

In terms of products available, domestic insurance companies has formulated policy clauses by drawing lessons from those of foreign insurance companies, and taking into account conditions in the domestic market and regulatory requirements. They are also actively exploring standardized and easy-to-replicate business models. On the one hand, they study the scenarios of cyber insurance. At the early stage, most of the clauses of cyber insurance policies were determined after communication and negotiation between insurance companies and their clients. With the accumulation of practical experience, the clauses of cyber insurance policies are being formulated to address specific risk scenarios at present. Standardized insurance products are developed to meet specific insurance needs and improve efficiency in promotion. On the other hand, by starting from covering additional risks and leveraging main risks to promote cyber insurance, some insurance companies sell cyber insurance attached to home property insurance or as small-amount complimentary insurance.

In terms of integration, domestic property insurance companies actively seek cooperation with technical firms specializing in cybersecurity to promote the combination of insurance mechanisms and technical measures of cybersecurity, explore cyber risk insurance plans for Chinese enterprises, and thus enhance clients' acceptance of this new-type insurance. Since the launch of the first cyber insurance product in China, three common cooperation models have emerged and are discussed below. The first model binds "security services and insurance". In this model, cybersecurity enterprises leverage their technological strengths to

power the main steps, such as insurance underwriting, loss mitigation, and claim handling through traditional technical means, such as risk assessment, risk monitoring, and emergency response. At the same time, insurance companies take the lead in insurance product development, risk loss quantification and underwriting and pricing, and comprehensively control risks of underwriting. For example, Zhongan Insurance and DAS-Security jointly launched comprehensive insurance plans for network and information security in 2017. Before that, DAS-Security sent a specialized security service team to form a risk assessment group with other members from Zhongan Insurance. After in-depth investigation and study of information security loopholes and possible risks within potential clients, they identified the severity of risks through risk assessment and controlled the risks with appropriate control objectives and methods. They provided users with a cybersecurity solution featuring "technical prevention and control + post-incident compensation". The second model combines "cybersecurity protection products + insurance". This model centers on the promotion of traditional cybersecurity services or protection products counters risks with insurance, and is included in enterprise risk management systems. In this model, sales motivation and enterprise-wide risk awareness level becomes the key to promotion. For example, in 2018, Qianhai Property & Casualty cooperated with NSFOCUS to launch comprehensive cyber insurance, which mainly provided a service mechanism of "insurance + security service", in which NSFOCUS provided technical services, such as information security assessment and emergency response, for enterprises, while Qianhai Property & Casualty provided financial safeguards in terms of additional costs and external liability compensation for enterprises. The third model is a whole-process "prevention + protection" cyber risk solution. In this model, insurance companies and insurance technology companies jointly develop cyber insurance plans by combining cybersecurity threat models with

insurance pricing models and underwriting scopes. They build quantitative risk assessment models for cybersecurity based on their advantages in data integration and analysis to improve the underwriting and pricing capabilities of insurance companies. At the same time, it provides active risk prevention services for enterprises to reduce the probability of cybersecurity incidents through continuous and periodic cybersecurity services, such as periodical inspection, fortification, monitoring, early warning, protection, and recovery. For example, 360 Government and Enterprise Security Group and China Life Property jointly launched the "Worry-Free Network" cyber insurance, which addresses cyber risks in an end-to-end manner by relying on insurance for cybersecurity and embedding whole-process risk management services.

Table 1. Overview of Cooperation between Large Cybersecurity Enterprises and Insurance Companies in China

Cybersecurity enterprise	Insurance company	Start of cooperation	Insurance products	Main features
DAS-Security	Zhongan Insurance	2017	Comprehensive insurance for network and information security	Providing tailored insurance solutions for governments, enterprises and institutions with a maximum limit of RMB 3 million for 10 service scenarios.
	CPIC Property Insurance	2020	Cooperative R&D of cyber insurance risk system	Building closed-loop insurance solutions for pre-incident risk prevention and control and ex post facto risk compensation, focusing on solving the problems related to comprehensive cyber insurance, comprehensive insurance for cloud computing security and event security services and safeguards.
J.V.S	Ping An Casualty Insurance	2017	Ping An Cyber Insurance Program	Providing cybersecurity defense plans and crisis advisory services, and a variety of insurance coverage in terms of scope of protection
Bluedon	Ping An Casualty	2017	Comprehensive cyber insurance +	Providing a complete set of cybersecurity product and service

	Insurance		security service	system and security assessment for governments, enterprises and individuals, and insurance solutions for potential economic losses of clients facing cyber risks.
NSFOCUS	Qianhai Property & Casualty	2018	Comprehensive cyber insurance	Mainly providing a service mechanism of "insurance + security services"; with three safeguards be added in 2020 to expand the scope of protection, upgrade supporting technical services and wider risk coverage.
QI-ANXIN	PICC Property Insurance	2018	Network information security insurance	Predicting cyber risks of enterprises and designing corresponding insurance plans
Meichuang	Guoren P&C	2020	"Noya Anti-Blackmail System + insurance" solution	Focusing on protection against attacks by ransomware; Providing all-round protection by combining the Noya Anti-Blackmail System, this is based on zero trust system, and data asset insurance.
Yuanbao Tech	/	2020	Cyber insurance	Providing model development and technical services for cyber insurance products of insurance and reinsurance companies; also providing "health management services" with active risk monitoring and early warning for enterprises, and improves the overall risk management level of enterprises with cyber insurance.
360 Government and Enterprise Security Group	PICC Property Insurance	2020	Cyber Insurance Cooperation Project	Simulating cyber risks and liability risks faced by governments and enterprises and designing corresponding insurance plans
	China Life Property	2020	"Worry-Free Network" cyber insurance	Addressing cyber risks in an end-to-end manner by embedding whole-process risk management services.

In terms of demand in industries, enterprises in key industries, such as manufacturing, finance, health care, and information technology, are actively inquiring prices of cyber insurance considering factors, such as policies, group-wide compliance, risk management,

events, and risk management system construction, hoping to transfer their cyber risks through insurance. Such enterprises usually have one or more of the following characteristics: First, they belong to industries highly attractive to cyber attacks, such as finance and manufacturing; second, they are key information infrastructure operators, whose normal operation is directly related to the fundamental interests of the nation, so it is necessary to establish a comprehensive risk management system; third, there are foreign-invested enterprises, China-foreign joint ventures or Chinese enterprises with overseas business units which have purchased or plan to purchase cyber insurance and urge domestic business units to actively respond to compliance requirements and seek cyber insurance for transferring risks.

3. DEVELOPMENT OF COMMERCIAL PROPERTY INSURANCE

Property insurance refers to "a category of insurance that takes property and its related interests as the object of insurance and provides compensation with money or in kind for loss of property caused by covered incidents (Wei and Lin, 1999)[26]. Property insurance may be further defined in a broad sense or a narrow sense: property insurance in the broad sense includes property loss insurance, liability insurance and credit guarantee insurance; property insurance in the narrow sense refers to that with tangible property and its related interests as the object of insurance. According to the classification of property insurance in *Yearbooks of China Insurance*, property insurance falls into seven categories: motor vehicle insurance, commercial property insurance, freight insurance, liability insurance, agricultural insurance, and credit guarantee insurance. Commercial property insurance accounts for 3.61% of the revenues of property insurance[1], ranking third among the categories of property insurance.

Commercial property insurance takes property located at fixed addresses as the object of insurance. By insurance liabilities, commercial property insurance may be divided into three categories by risk: basic property insurance, comprehensive property insurance and all-risk property insurance. More, commercial property insurance may protect three types of property. The first is the property solely owned by policyholders or jointly owned by policyholders and other and being the responsibility of the policyholders; the second is the property that is managed or kept by policyholders on behalf of others, such as inventory; the third is the property in which the policyholders have economic interests recognized by law, such as property leased by policyholders. Specifically, the property may be divided into four categories, i.e., buildings, machinery and equipment, raw materials and inventory, and office appliances. The object of commercial property insurance only covers property is kept at fixed

[1] Source: Data on premiums in 2020 published by National Bureau of Statistics

places and remains relatively static, that is, fixed assets of enterprises.

3.1 Academic Research

Geographically, the academic research of commercial property insurance has largely taken place in developed countries such as those in Europe, the United States, Japan, and South Korea, where relatively mature property insurance markets exist. There is a limited base of literature on commercial property insurance in China, and most is based on the findings of existing studies conducted abroad as insurance market started late in China.

Huang (1994)[27] thought that the property insurance in China cannot meet the needs of enterprises for "insurance commodities" due to their characters of concentrated risks, high premiums, and limited types, and put forward suggestions on the reform and development of main types of insurance. Gao and Yin (1999)[28] discussed the necessity, feasibility, methods and steps of changing the underwriting practices of commercial property insurance based on the actual conditions in Shandong Province. Shi (1999)[29] suggested that maintaining property insurance is the fundamental approach of enterprises in development of production and operation and response to disasters by analyzing the actual conditions in Shanxi Province. Chen (2005)[30] explained the effect of property insurance promoting the value of enterprises from several aspects, such as reduction of financing costs and expected tax payment, and the reduction of possibility of falling into financial difficulties. Su (2007)[31] pointed out that China's private economy had been developing rapidly, but the property insurance for private enterprises had lagged behind, mainly because certain problems within private enterprises had impeded the supply and demand of insurance. Zhu and Kui (2009)[32] analyzed the effect of bankruptcy costs, shareholder-manager game, shareholder-creditor game, tax policy and industry regulations on the demand for commercial property insurance in China. Yan and Su (2012)[33] identified problems to be addressed in property insurance management, including:

correctly understanding the relationship between insurance and preventive measures; properly handling the balance between premiums and cost control; focusing on solving the gap between insurance purchase and insurance management.

The early studies mainly focused on theoretical research as an important part of enterprise risk management. With the improvement of the theoretical framework of demand for commercial property insurance, most recent studies have explored the factors affecting demand for commercial property insurance through empirical research.

Zou, Adams et al. (2003)[34] found that the prevention of bankruptcy risks is the main factor affecting the demand for property insurance from a sample of 235 listed companies in China from 1997 to 1999. They also noted that larger enterprises are more willing to purchase property insurance, but there are only a small number of enterprises doing so. In addition, those in inland cities are more likely to purchase property insurance than those in coastal cities. Zou and Adams (2006)[35] introduced some variables based on the previous model. The results show that the financial leverage, managers' shareholding ratio, growth opportunities, proportion of tangible assets and the effective tax rate have a positive impact on the demand for property insurance. Government subsidies have little effect on the demand for commercial property insurance, and even reduce the demand for commercial property insurance to a certain extent. They (Zou and Adams, 2009)[36] also found that the purchase of commercial property insurance by Chinese listed companies reduced the default risk of corporate debts, thus improving the borrowing ability of enterprises and making the debt costs of enterprises lower than the those when they do not buy commercial property insurance.

For commercial property insurance in China, domestic and foreign scholars have found identified the main factors affecting the demand for commercial property insurance, including those for preventing bankruptcy risks (Zou, Adams et al., 2003)[34], fixed assets

investment (Song, 2008; Zhao and Su, 2013)[37][39], effective tax rate (Zhu, Lu et al., 2010; Huang and Zhang, 2014)[38][40], financial leverage (Zou, Adams et al., 2003; Huang and Zhang, 2014)[34][40], enterprise scale (Yang, Zhong et al., 2010; Yang, Yu et al., 2010)[41][42], percentage of tangible assets (Yang, Zhong et al., 2010; Xiao, Liu et al., 2021)[41][43], education level (Zhao and Su, 2013; Ju and Xue, 2021)[44][45].

3.2 Market Development

Property insurance companies in China mainly engaged in insurance for cargo transportation before 1949. After the founding of the New China, all enterprises were state-owned. To meet the needs for developing the New China, the State Council released the *Decision on Implementing Compulsory Property Insurance and Compulsory Passenger Insurance for State Organs, State-owned Enterprises and Cooperatives*[2] in 1951, and commercial property insurance was generally purchased by major state-owned enterprises as a compulsory insurance plan. Commercial property insurance was the fastest growing field of insurance since the insurance sector was resumed in 1979 (Liu, 2017)[46]. In the mid-1980s, the premiums of commercial property insurance already reached RMB 1 billion, accounting for 50% of the premiums of property insurance. However, commercial property insurance shrunk relatively since the late 1980s. Though the national GDP kept growing at an average annual rate of 9%, the average annual growth rate of fixed assets investment and that of added value of the secondary sector stayed above 10%, the growth of commercial property insurance failed to keep pace with the economic development. In terms of the growth of property insurance after enter into the 21st century (See Figure 1), the total premiums of property insurance have been expanding. The total premiums of property insurance were RMB 60.8 billion in 2000 and increased to RMB 1,358.369 billion in 2020, an increase of

[2] Source: http://hprc.cssn.cn/gsgl/dsnb/dsj/dsj1951/200906/t20090627_3949513.html

2,134.16%. The growth rate in 2010 reached 25.68%, the highest in recent 20 years, according to Figure 1. The growth rate of total premiums of property insurance slowed to only 4.18% in 2020[3].

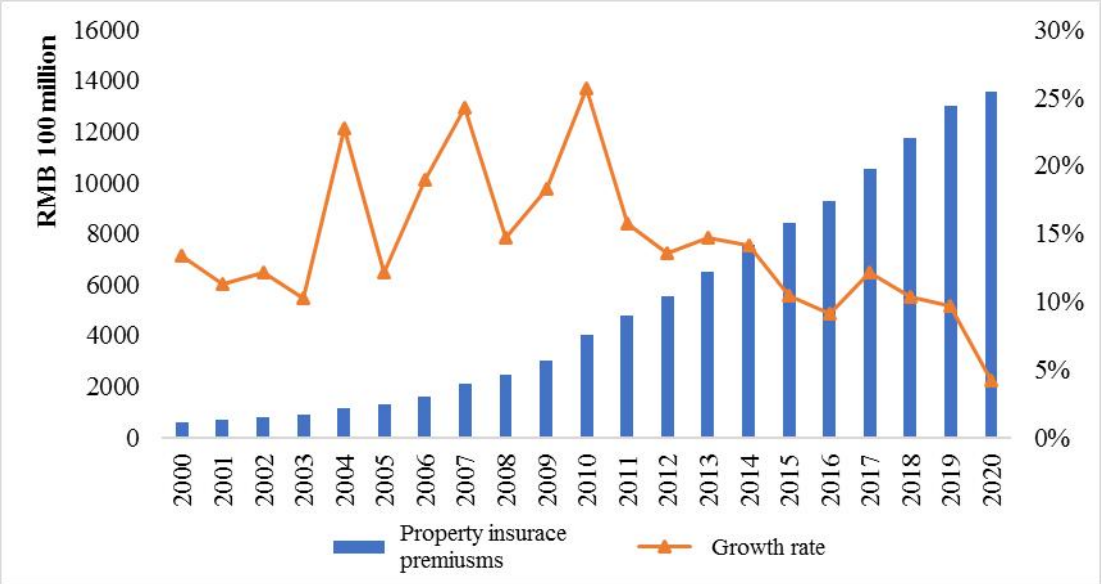


Figure 1. Premiums of Property Insurance in China from 2000 to 2020

In terms of commercial property insurance premiums (See Figure 2), the total premiums of commercial property insurance kept increasing from 2000 to 2020. The total premiums of commercial property insurance increased from RMB 11.8 billion in 2000 to RMB 49.026 billion in 2020, an increase of 315.47%. However, the growth rate undulated noticeably, especially in 2016, when the growth rate was -1.31%.

[3] Source: Premiums data of National Bureau of Statistics, https://data.stats.gov.cn/easyquery.htm?cn=C01&zb=A0L0E01&sj=2021

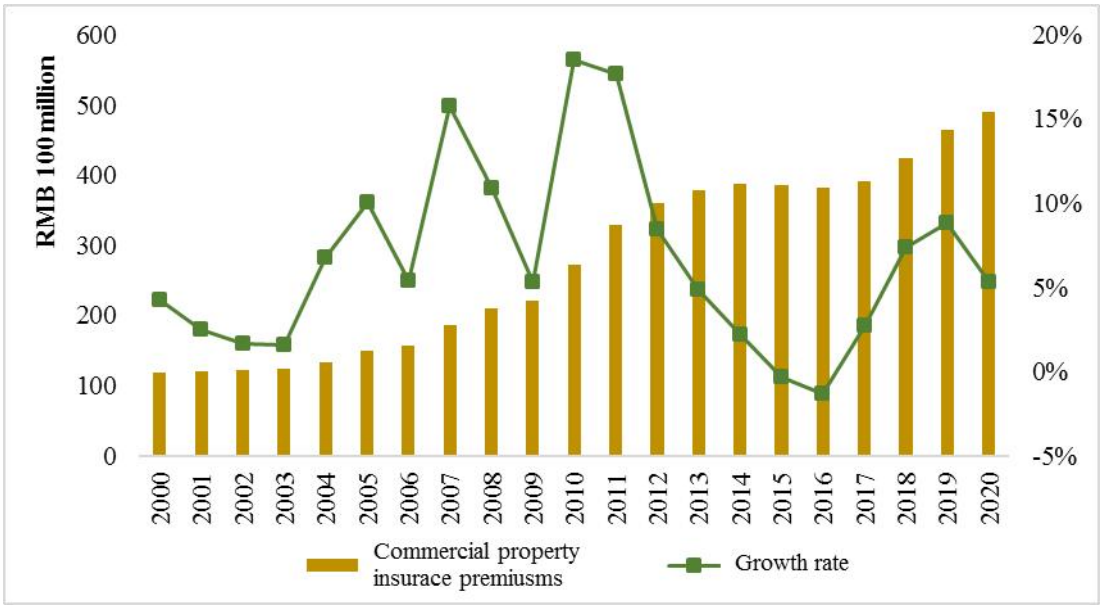


Figure 2. Premiums of Commercial Property Insurance in China from 2000 to 2022

It is worth noting that the percentage of commercial property insurance in property insurance is diminishing (See Figure 3). Premiums of commercial property insurance accounted for 19.41% of premiums of property insurance in 2000 and 3.61% in 2020, through this percentage trends to stabilize.

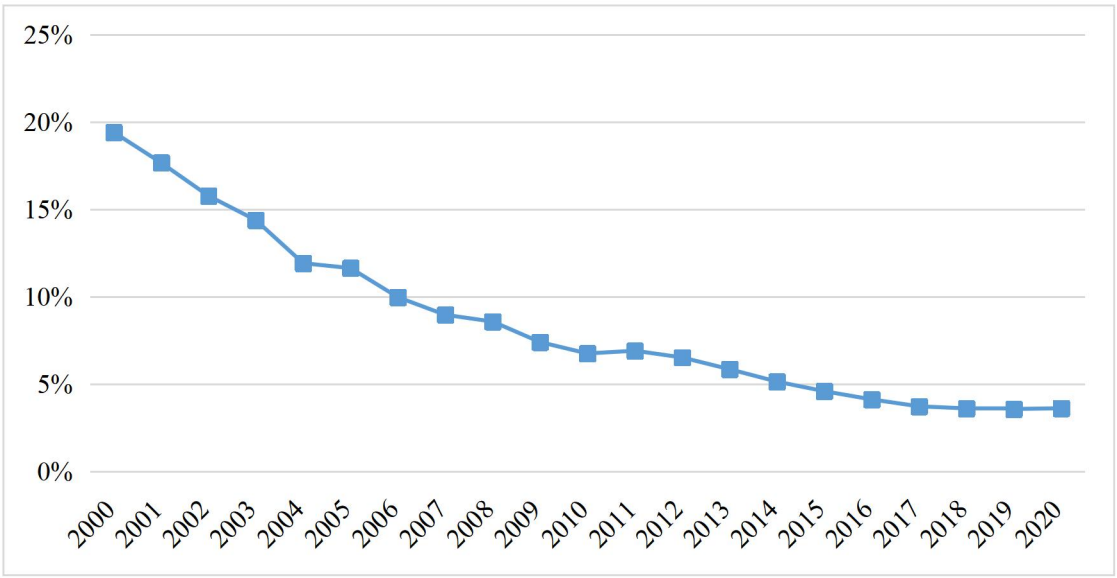


Figure 3. Percentage of Commercial Property Insurance in Property Insurance from 2000 to 2020

4. EXPLORATION OF COMBINATION OF CYBER INSURANCE AND COMMERCIAL PROPERTY INSURANCE

4.1 Feasibility Of Combining Cyber Insurance With Commercial Property Insurance

The continuous expansion of the cybersecurity market, continuous improvement in top-level cybersecurity laws and regulations, and establishment of cyber insurance ecosystem have provided favorable market, legal and institutional conditions for the development of cyber insurance and commercial property insurance with higher possibility for the combination of the two categories of insurance.

4.1.1 Frequent Cybersecurity Incidents And Expanding Cybersecurity Market

China's digital economy reached RMB 39.2 trillion in 2020, accounting for 38.6% of GDP, as the new-type information infrastructure has gradually become a new driver of economic growth, including that for 5G, artificial intelligence, Internet of Things, industrial Internet, and satellite Internet[4]. Highly frequent digital interactions have given rise to new cyber risks along with the rapid development of digital economy. According to the "China's Internet Cybersecurity Situation Report" released by the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT) (See Figure 4), the China National Vulnerability Database (CNVD) recorded 20,704 general software and hardware vulnerabilities in 2020, an increase of 27.9% compared with 2019[5]. Cybersecurity incidents caused by vulnerabilities are not uncommon. For example, 16.79 million entries of data of a domestic bank were leaked in January; SMS phishing attacks occurred against rural credit cooperatives and urban commercial banks in February; hackers invaded systems of Acer, a PC manufacturer in Taiwan, China, and demanded a ransom of USD 50 million in March; nearly 1.2 billion user data of Taobao was leaked in June; a major computer company

[4] Source: https://www.isc.org.cn/article/40203.html
[5] Source: http://www.cnnvd.org.cn/web/vulreport/queryListByType.tag?qnewtype=2

in Taiwan Province, China, was attacked by ransomware, and hundreds of GB of data were stolen in August. All these incidents suggest the urgency for strengthening cybersecurity.

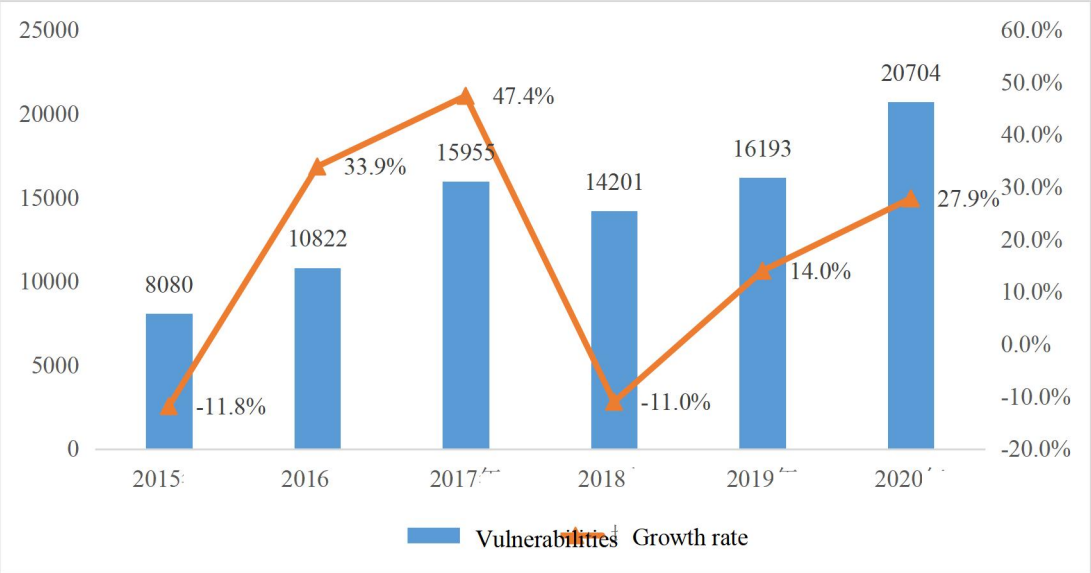


Figure 4. Number of Cybersecurity Vulnerabilities Recorded in CNVD from 2015 to 2020

The scale of the cybersecurity industry together with the market demand has kept expanding as a result of the growing digital economy and frequent occurrence of cybersecurity incidents. According to the statistics of the China Academy of Information and Communication Technology[6], the scale of China's cybersecurity industry reached RMB 172.93 billion in 2020, an increase of 10.6% compared with 2019, and is expected to reach about RMB 200.25 billion in 2021, with an increase of about 15.8%.

[6] Source: Summary of data in "White Paper on China's Cybersecurity Industry" released by the China Academy of Information and Communication Technology

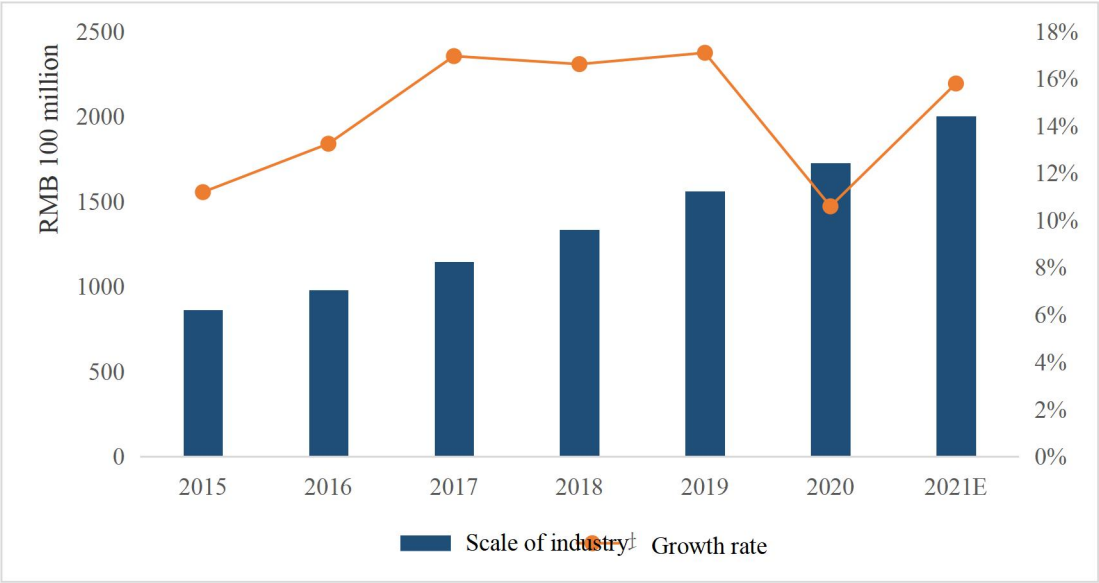


Figure 5. Growth of China's Cybersecurity Industry from 2015 to 2021

The revenues of China's cybersecurity industry have increased synchronously with the growth of market (See Figure 6). According to the statistics of the China Cybersecurity Industry Alliance[7], China's cybersecurity market reached about RMB 53.2 billion in 2020. Affected by COVID-19, the growth rate of cybersecurity market slowed down in 2020, with a year-on-year increase of 11.3%. It is estimated that the cybersecurity market will maintain a growth rate of over 15% from 2022 to 2023, and the market size will exceed RMB 80 billion by 2023.

[7] Source: http://www.china-cia.org.cn/home/WorkDetail?id=61ca800a0200330f80e90e94

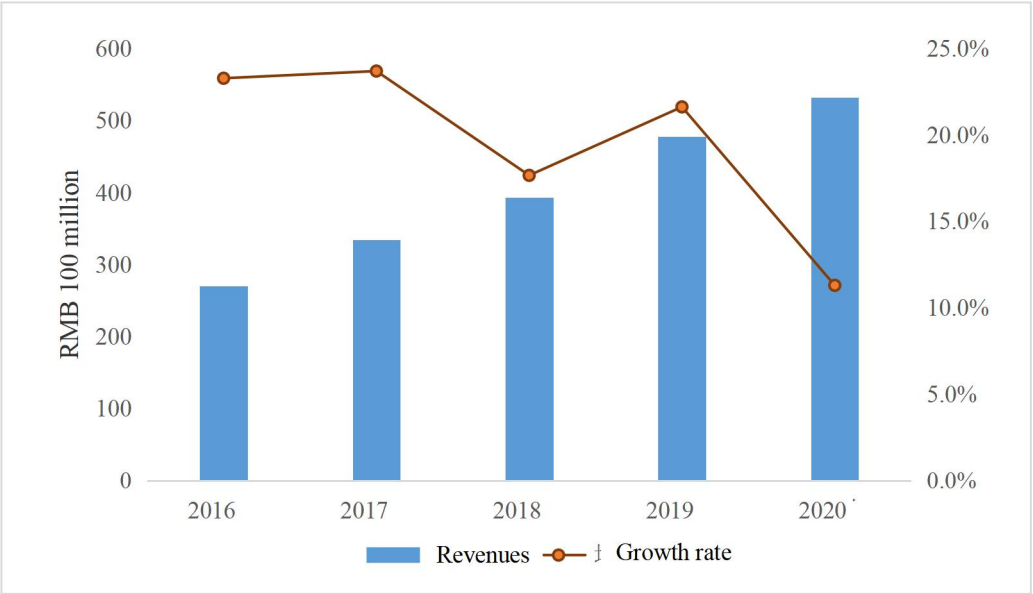


Figure 6. Revenues of China's Cybersecurity Market from 2016 to 2020

As for procurement[8], 51,505 bidding announcements for cybersecurity projects were released with a total budget of about RMB 126.498 billion from 2019 to 2021 according to incomplete statistics. Among them, 15,297 bidding announcements were released with a total budget of about RMB 38.259 billion in 2019; 17,633 bidding announcements were released with a total budget of about RMB 41.664 billion in 2020; 18,575 bidding announcements were released with a total budget of about RMB 46.575 billion in 2021. In addition, data of ccgp.gov.cn (Chinese Government Procurement Portal)[9] show 429 contracts were signed for cybersecurity-related projects with a total contract value of RMB 511 million in 2019; 517 contracts were signed for projects with a total contract value of RMB 1.168 billion in 2020; 874 contracts were signed for projects with a total contract value of RMB 2.762 billion in 2021. Both the number of projects and contract value kept rising over the years.

[8] Source: Collated with data from zhaobiaoziyuan.com
[9] Source: Collated with data from ccgp.gov.cn (Chinese Government Procurement Portal), http://htgs.ccgp.gov.cn/GS8/contractpublish/search?contractSign=0

4.1.2 Continuous Improvement in Top-Level Design and Release of Favorable Industrial Policies

In the insurance sector, the *Insurance Law of the PRC* was adopted in 1995 and revised for the third time in April 2015, further clarifying the rights and obligations of parties involved in insurance activities, strengthening the protection of policyholders, and further completing the basic rules of the insurance sector. Regulations and policies to promote implementation of the law include the *Opinions on Reform and Development of Insurance Industry* released by the State Council in 2006, *Circular on Issues Related to Acceptance upon Opening of Specialized Network Insurance Companies* released by the China Insurance Regulatory Commission in 2013, the *Three-year Action Plan for High-quality Development of Network Security Industry (2021-2023) (Draft for Comments)* released in July 2021, and the *14th Five-Year Development Plan of Insurance Technology* released by the Insurance Association of China issued in 2022, emphasizing expansion of the service scope of the insurance sector, improvement of the insurance market system, optimization of insurance service models, and collaboration of insurance service institutions to develop appropriate and high-quality network risk insurance products and carry out pilot cyber insurance services.

The adoption of laws, such as the Cybersecurity Law of the PRC, Data Security Law of the PRC, and Personal Information Protection Law of the PRC, have gradually improved China's cybersecurity legal system with clearly defined the responsibilities of cybersecurity entities, obligations for data protection, etc., and laid a sound legal foundation for the development of cyber insurance in China. The *Guidelines for Promoting the Development of Cybersecurity Industry (Draft for Comment)* and the *Three-year Action Plan for High-quality Development of Network Security Industry (2021-2023) (Draft for Comments)* released by the Ministry of Industry and Information Technology, and the *14th Five-Year Development Plan*

of Insurance Technology released by the Insurance Association of China and other policy documents clearly require pilot implementation of cyber insurance services and explore cyber insurance services. Such favorable industrial policies have been continuously released, laying an institutional foundation for its high-quality development. In addition, China Cybersecurity Industry Alliance released the *Guide to Implementation of Security Risk Assessment for Cyber Insurance (Draft for Comment)* to guide insurance companies and reinsurance companies to conduct risk assessment and risk pricing before starting the cyber insurance business by establishing a set of risk assessment indicators and processes. It also provides information for cyber insurance policyholders or purchasers to conduct self-assessment of cyber risks.

Table 2. Summary of Laws and Policies Related to Development of Cyber Insurance in China

Time	Law/regulation/policy	Relevant provisions
June 2006	Opinions of the State Council on Reform and Development of Insurance Industry	The document requires broadening the range of insurance services and improving the insurance market system and building an insurance innovation mechanism oriented to market demand and combining with learning and independent innovation.
August 2013	Circular on Issues Related to Acceptance upon Opening of Specialized Network Insurance Companies	Additional specifically applicable clauses are added with respect to the opening acceptance of specialized network insurance companies based on the Guidelines on Acceptance upon Opening of Insurance Companies.
October 2013	Consumer Protection Law of the People's Republic of China	The law provides for the rights of consumers, the obligations of business operators, the protection of consumers' legitimate rights and interests by the state, consumer organizations, dispute resolution and legal responsibilities.
April 2015	Insurance Law of the People's Republic of China, amended	The law further clarifies the rights and obligations of the parties involved in insurance activities and strengthens the protection of interests of policyholders; improves the basic system of the insurance industry; enhances the self-discipline of the insurance sector; defines the responsibilities of insurance regulatory agencies, strengthens regulatory means and measures, clarifies legal responsibilities, and crack down on violations in insurance.

November 2016	Cybersecurity Law of the Republic of China	The law is intended to ensure cybersecurity and promote the healthy development of economic and social informatization.
April 2020	Measures for Cybersecurity Review	Network products or services that affect or may affect national security shall be subject to cybersecurity review.
January 2021	Civil Code of the People's Republic of China	The code contains basic provisions on contracts.
June 2021	Data Security Law of the Republic of China	The law establishes and improves the national data security management system and improves the data security governance system.
August 2021	Personal Information Protection Law of the People's Republic of China	The law establishes the "notification-consent" principle as the core requirement in processing personal information, and requires corresponding security technical measures to protect personal information.
July 2021	Three-year Action Plan for High-quality Development of Network Security Industry (2021-2023) (Draft for Comments)	The document requires pilot implementation of cyber insurance services in fields, such as telecommunications and Internet, industrial Internet and Internet of Vehicles, and acceleration of the policy guidance and standard formulation for cyber insurance. It also requires monitoring risk exposure through cyber insurance services and encourages enterprises to build and improve their own cyber risk management systems and strengthen their ability in coping with cyber risks.
September 2021	Regulations on Security and Protection of Key Information Infrastructure	The regulation clarifies the supervision and management system, and clarifies the responsibilities and obligations of operators, legal responsibilities and other elements.
December 2021	14th Five-Year Development Plan of Insurance Technology	The plan requires optimizing insurance service models, providing diverse insurance products, expanding the coverage of insurance services, improving the quality and efficiency of the insurance supply system, building a complete-chain ecosystem of insurance, and driving the objective needs of high-quality development of the insurance sector.

4.1.3 In-Depth Collaboration between Service Enterprises in Actively Building a New Ecosystem

Third-party risk management and technical service institutions, such as cybersecurity

companies and insurance technology companies, actively leverage their specialized advantages in providing two-way risk management services to insurers and policyholders, and deeply participate in building an ecosystem of the property insurance industry for cybersecurity. Among them, insurance companies are expanding presence in terms of product design, technical services, business models, etc., while cybersecurity companies are assisting insurers and policyholders in reviewing the risk accumulation level and implementing cyber risk management and control by leveraging their specialized capabilities of cybersecurity technology, scenario assessment and analysis, and data integration and analysis. In addition, to address problems, such as insufficient insurance demand and limited risk management and control capability of enterprises, insurance companies, security service providers, third-party technical service providers for risk management, and other market entities cooperate deeply to optimize the supply of products and services, strengthen the role of cybersecurity property insurance in driving demand, promote the standardization of cybersecurity property insurance services, and build a benign property insurance ecosystem for cybersecurity.

4.2 Necessity Of Combining Cyber Insurance With Commercial Property Insurance

4.2.1 Driving With Internal Factors Of The Insurance Industry

On the one hand, the demand side lacks motivation to purchase cyber insurance, while the market of commercial property insurance is large, and insurance companies have rich experience in promoting commercial property insurance. Combining these two categories could promote the expansion of cyber insurance through the scale effect of commercial property insurance.

On the demand side, most enterprise little about cyber insurance and are unlikely to accept transferring cyber risks through insurance. A possible reason is lack of attention to cyber risk management. At present, enterprises generally neglect security in the process of

development, and just take "compliance" as the standard in cybersecurity plans. According to the data of Munich Re[10], enterprises are investing far more in cybersecurity technology than in cyber insurance. This suggests that they pay more attention to the deployment of cybersecurity equipment and technology for front-end mitigation. Enterprises seldom implement risk monitoring, control and management measures from the perspective of risk reduction, and invest in comprehensive planning of cyber risk management and post-event response mechanism.

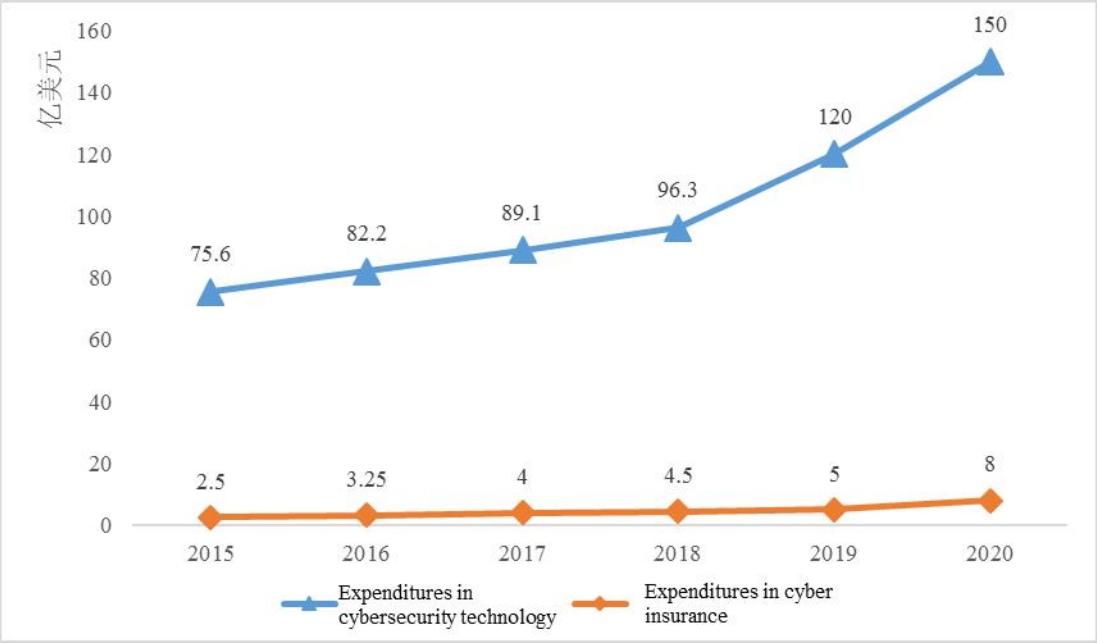


Figure 7. Comparison of Expenditures in Cybersecurity Technology and Cyber Insurance around the World from 2015 to 2020

Another reason is the lack of understanding of cyber insurance. At present, many clients, especially small and medium-sized companies, are unfamiliar with relevant products or their own needs as effective ways available are limited for promoting cyber insurance (Zhang, 2022)[47]. Most enterprises simply deem cyber insurance as a way of getting compensation after damages occur. Some enterprises know cyber insurance helps reduce

[10] Source: Munich Re, Gartner

compliance risks or enhance credit standing, while having almost no knowledge about the risk management services provided simultaneously. The management is unlikely to invest enough time and other resources in cybersecurity when they lack awareness of cybersecurity, because it is difficult to prove cybersecurity's value (Philpot, 2021)[48].

These factors result in the fact that the number of cyber insurance policies underwritten is small, which leads to insufficient risk diversification of insurance companies and lack of support from reinsurance for risk diversification (Xu, 2022)[1]. Therefore, insurance companies need to find new marketing models by taking cyber insurance as a category of commercial property insurance to expand the market of cyber insurance.

On the other hand, in the context of digital transformation, commercial property insurance cannot meet the needs for risk transfer for new-type assets, while cyber insurance provides the means of risk transfer for networks, data and other assets. The combination of the two can diversify commercial property insurance and meet the market demand. Assets are physical or virtual forms of capital, and are carriers of underwriting risks of commercial property insurance (Lu and Wang, 2020)[49]. At present, commercial property insurance mainly includes four categories, i.e. basic insurance, comprehensive insurance, property insurance, and all-risk insurance. The object of insurance only covers property kept at fixed places and in a relatively static state, i.e., fixed assets of enterprises. However, digitalization has become a new driver of the socialist market economy, driving the development of digital economy due to the advancement of modern digital information technologies, such as 5G, Internet, and Internet of Things, As a result of the high-level development of market economy and digital economy, and their joint impact, digital assets have become a new type of assets different from tangible assets and intangible assets (Lu, 2020)[50]. Digital assets stored in the virtual space are exposed to possible loopholes in technical design and external hacker

attacks. Compared with other assets, digital assets are faced with major risks of business interruption and data leakage in the era of digital economy (Lu and Zhou, 2020)[51]. Therefore, commercial property insurance cannot meet the needs for protecting such new assets of enterprises.

Coming to the rescue, cyber insurance is the "blood" of the digital economy security system and the ultimate means of risk transfer (Xu, 2022)[1]. It can be divided into two categories: first-party property loss insurance and third-party liability insurance. The former protects against direct financial losses caused by data asset loss and is used in enterprise crisis management, business interruption, data asset protection, ransomware on network and other fields (Eling and Schnell, 2016)[52]. The latter is to protect against third-party liability caused by data loss. Typical covered liabilities include privacy liability, cybersecurity liability, intellectual property rights, media leakage liability, etc. (Kshetri, 2010)[53].

As a result, insurance companies should focus on meeting client needs and improving enterprise efficiency in the longer term by expand the coverage of liabilities to increase products' competitiveness and meet the needs of enterprises.

4.2.2 External Environmental Impact from COVID-19

The COVID-19 pandemic has swept around the world since 2020. On the one hand, the "online business" of insurance companies will inevitably change to the business models, performance and client experience of insurance (Yan and Du, 2020)[54]. China's commercial insurance premiums, monthly year-on-year growth of premiums, insurance density and insurance depth have all declined due to COVID-19 (Wang, Zhang et al. 2020)[55]. Meanwhile, cyber risks faced by enterprises have increased as many previously offline activities have been performed online to in various industries. In view of the impact of COVID-19 in the insurance sector, the General Office of the China Banking and Insurance Regulatory

Commission released the *Circular on Further Improving Financial Services in Epidemic Prevention and Control* (YBJBF [2020] No. 15)[11] in February 2020, which required insurance companies to enhance the expansion of commercial property insurance and workplace safety liability insurance to provide better safeguards for the production and operation of enterprises. The circular also actively urged and encouraged insurance companies to develop insurance products that meet the challenges caused by COVID-19 and conform to insurance principles, and innovate methods in insurance service by applying modern scientific and technological means. In academia, as economic activities recover gradually in the post-COVID era, scholars believe that the growth of direct insurance premiums will take a V-shape and product innovation and technological innovation will be main factors influencing the insurance sector (Chu and Dang, 2021)[56]. They also suggest that China's insurance sector should actively explore innovation of insurance technology and other measures to turn more uninsurable risks into insurable ones (Li and Cheng, 2020)[57], by, for example, combining cyber insurance with insurance technology to explore new opportunities brought by insurance technology to cyber insurance (Tang and Mo, 2022)[12]. Therefore, the combination of cyber insurance and commercial property insurance as cyber property insurance not only responds to the requirement for innovation of insurance services, but also meets the needs of enterprises for transfer of cyber risk, providing more comprehensive high-quality protection for the production and operation of enterprises in the post-COVID era.

4.3 Projection Of Cybersecurity Property Insurance Market

1) Model Setup

The value of cybersecurity property insurance for enterprises is to compensate for

[11] Source: http://www.gov.cn/zhengce/zhengceku/2020-02/16/content_5479561.htm

their possible losses, and the utility that enterprises can obtain by purchasing the insurance is related to their risk level. In addition, there is a certain relationship between the premiums of cybersecurity property insurance P, the revenues of cybersecurity market W, the demand of enterprise for cybersecurity property insurance Q and the cyber risk losses suffered by enterprises S. Therefore, the following hypothetical model is established to comprehensively predict the market scale of cyber insurance premiums:

$$\boldsymbol{P = \alpha W + \beta Q + \gamma S} \quad (1)$$

Model variable description:

Variable	Description
$\boldsymbol{P}$	Premiums of cyber insurance
$\boldsymbol{W}$	Revenues of the cybersecurity market
$\boldsymbol{Q}$	Demand for enterprise cybersecurity property insurance
$\boldsymbol{S}$	Enterprise cyber risk losses
$\boldsymbol{\alpha}$	Stands for factors affecting the cybersecurity market, including cybersecurity environment (such as network vulnerabilities, number of malicious programs, etc.), advanced technology of cybersecurity defense, and the impact of national cybersecurity policies and regulations
$\boldsymbol{\beta}$	Stands for factors affecting the demand of enterprises for cyber insurance, including cybersecurity threats (such as data leakage, malicious attacks, etc.) faced by enterprises, enterprise size, and proportion of tangible assets
$\boldsymbol{\gamma}$	Stands for factors affecting the losses, including value of assets, network scale, and investment in cybersecurity defense

2) Variable Selection and Data Sources

(1) Premiums of cybersecurity property insurance

This paper discusses cybersecurity property insurance which combines cyber insurance and enterprise property insurance and its promotion as a type of enterprise property insurance. Due to the rareness of data on premiums of cyber insurance and cybersecurity property insurance in China, the data on enterprise property insurance from the National Bureau of Statistics is used to represent the premiums of cybersecurity property insurance as premiums of enterprise property insurance and premiums of cybersecurity property insurance share the same trend.

(2) Revenues of the cybersecurity market

In this paper, the statistics from China Cybersecurity Industry Alliance from 2015 to 2020 are used as the data sample for research.

(3) Demand for enterprise cybersecurity property insurance

In this paper, the primary purpose of cybersecurity property insurance is to keep data confidentiality and cybersecurity. On the one hand, the insured would suffer financial losses if data leakage or loss happens. Vulnerabilities in cybersecurity are likely to result in direct losses to the insured, such as direct costs caused by system crash or service interruption, financial losses or recovery costs caused by Internet fraud or blackmailing, repair costs caused by virus transmission, and loss of profits caused by the aforementioned incidents. That is, the demand for enterprise cybersecurity property insurance is mainly reflected in the number of malicious computer program samples, the weight of malicious program samples on the mobile Internet, the number of security vulnerabilities, etc. Moreover, no statistics on the demand for enterprise cybersecurity property insurance in China is available at present.

Therefore, in this paper, the number of malicious computer program samples, the number of malicious programs on mobile Internet and the number of security vulnerabilities in the *China Internet Network Security Report* are used to represent the demand for cybersecurity property insurance.

(4) Enterprise cyber risk losses

Enterprises may suffer direct and indirect losses arising from cybersecurity risks. Direct losses include, for example, costs caused by system crash or service interruption, financial losses or recovery costs caused by Internet fraud or blackmailing, repair costs caused by virus transmission, and loss of profits caused by the aforementioned incidents, while indirect losses include, for example, legal liabilities caused by the spread of computer viruses, costs of public relations and media in case of crises, costs of increased credit and identity monitoring services to reduce future losses of customers, costs of taking responsibility for violating laws and regulations. When an enterprise is exposed to network risks, the most possible direct consequences include invasion of servers or hosts by malicious programs, tampering with or counterfeiting of enterprise websites, and implanting of back doors. Moreover, no statistics on enterprise cyber risk losses in China is directly available at present. In this paper, the number of malicious programs taking control of servers and hosts, the number of websites being tampered with or counterfeited and the number of implanted back doors in the *China Internet Network Security Report* are used to represent the network risk losses of enterprises. The selected data of the above variables are summarized in the following table:

Table 3. Summary of Analytical Data

Year	Premiums of cybersecurity property insurance (RMB 100 million)	Revenues of cybersecurity market (RMB 100 million)	Demand for enterprise cybersecurity property insurance	Enterprise cyber risk losses
2015	7994.97	2190	13851.87	900.06
2016	8724.17	2700	14532.35	1360.84
2017	9834.57	3340	14652.48	1496.59
2018	10770.69	3930	13419.19	1921.36
2019	11649.47	4780	14414.84	2621.42
2020	11928.58	5320	18060.41	2911.76

3) Sample Data Description

Only relevant data from 2015 to 2020 are collected due to the insufficiency of data on the premiums of cyber insurance (P), demand for enterprise cybersecurity property insurance (Q), and enterprise cyber risk losses (S) in China. The main reasons are that, first, few enterprises disclose information on security needs and security losses; second, few organizations in China collect and collate data on cybersecurity incidents; third, government statistics are relatively obsolete in China.

The small sample size of statistics may affect the results of regression analysis. For example, a greater effect of random deviating data in statistics would lead to biased research results. Nevertheless, the exemplary linear regression for the projection model in this paper presents relevant ideas and processes (such as variance analysis, significance analysis, and residual normality test). Though the results have no statistical significance at present, satisfactory results are expected through linear regression with the model when relevant databases are established with sufficient data to support statistical analysis in China.

4) Model Prediction

As a tool for risk transfer, the value of cybersecurity property insurance for

enterprises is to compensate for their possible losses. The demand for enterprise cybersecurity property insurance is related to the extent of losses that enterprises may suffer. That is, the higher the probability of losses or the more serious the consequences of losses, the greater the value of purchasing insurance. Insurance is desired to compensate for losses, thus increasing the premium income of insurance companies. Hence, the following hypothesis is made:

H1: Cybersecurity risk losses of enterprises are positively correlated with demand for cybersecurity property insurance. That is, the greater the cybersecurity risk losses enterprises may suffer, the greater the demand for cybersecurity property insurance.

From Figure 8, there is a strong correlation between the demand of enterprises for cybersecurity property insurance and the potential loss from cybersecurity risks. The higher the potential loss from cybersecurity risks, the greater the demand for cybersecurity property insurance. The cybersecurity risks faced by enterprises include, for example, internal technical and management risks as well as risks related to the external physical environment, network architecture, network operation and maintenance, etc. Generally, enterprises with higher levels of informatization are faced with more types of cybersecurity risks. Failure to take appropriate measures for evading or reducing the probability of risks may cause incalculable losses to enterprises. By purchasing cybersecurity property insurance at small fixed expenses every year, they can reduce the losses caused by cybersecurity threats, such as unavailability of information equipment, business interruption, and information leakage, reduce the cost of responding to cybersecurity accidents, and improve the ability of post-disaster recovery.

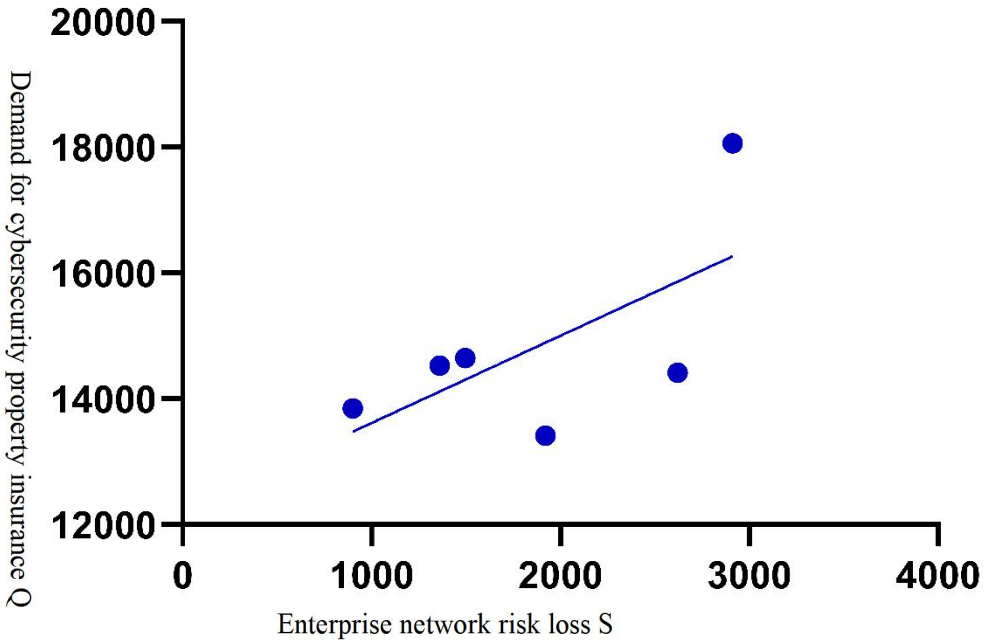


Figure 8. Relationship between cybersecurity risk losses of enterprises and demand for enterprise cybersecurity property insurance

The possible cybersecurity risk losses of enterprises drive the increase in revenues of the cybersecurity market and premiums of cybersecurity property insurance. On the one hand, enterprises take defensive measures to manage cyber risks, such as deploying and installing security equipment and software against firewalls and intrusion prevention to reduce possible losses caused by network attacks. On the other hand, enterprises transfer the remaining cyber risks by purchasing cyber insurance products because network and information security defense technologies are developed in response to hackers' application of cutting-edge network technologies and they are always in a passive position. Accordingly, the following hypothesis is made:

H2: Cybersecurity risk losses of enterprises are positively correlated with

revenues of the cybersecurity market and premiums of cybersecurity property insurance. That is, the greater the cybersecurity risk losses enterprises may suffer, the higher the revenues of the cybersecurity market and the premiums of cybersecurity property insurance.

From Figure 9, there is a strong linear correlation between losses of enterprise from cybersecurity risks and the revenues of the cybersecurity market and the premiums of cybersecurity property insurance. When enterprise managers become aware of the cybersecurity risks faced by their enterprises and potential losses to be caused by such risks, they usually make necessary investments in the management of network risks to protect the assets and ensure the long-term development of enterprises. If they choose to resist the risks of network intrusion by purchasing cybersecurity products or services, the scale of the cybersecurity market tends to expand accordingly; if they try to transfer the remaining cybersecurity risks by purchasing cybersecurity property insurance, they contribute to the increase of premiums of cybersecurity property insurance.

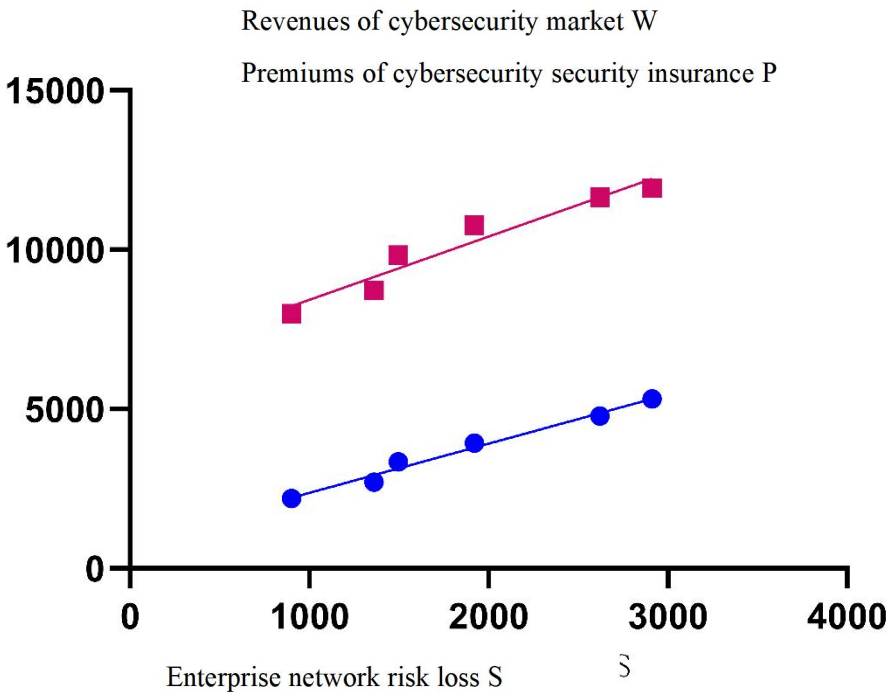


Figure 9. Relationship between cybersecurity risk losses of enterprises and revenues of the cybersecurity market and premiums of cybersecurity property insurance

According to the relevant data from the National Bureau of Statistics and the China Cybersecurity Industry Alliance, the revenues of the cybersecurity industry and premiums of enterprise property insurance kept increasing from 2015 to 2020. The revenues of the cybersecurity industry increased from RMB 21.9 billion in 2015 to RMB 53.2 billion in 2020; The premiums of enterprise property insurance increased from RMB 799.497 billion to RMB 1,192.857 billion in the same period. Hence, the following hypothesis is made:

H3: Revenues of the cybersecurity industry are positively correlated to premiums of cybersecurity property insurance. That is, the larger the revenues of the

cybersecurity market, the higher the premium income of insurance companies.

From Figure 10, there is a strong linear fit between the premiums of cybersecurity property insurance and the revenues of the cybersecurity industry. On the one hand, when the cybersecurity property insurance covers cybersecurity products or services, i.e. cybersecurity software and hardware, equipment, or services purchased by enterprises to avoid network risks, enterprises would include such software and hardware, equipment, or services in the scope of the purchased cybersecurity property insurance. As a result, with more cybersecurity software and hardware, enterprises are likely to pay higher premiums of cybersecurity property insurance. On the other hand, as a combination of cybersecurity insurance and enterprise property insurance, cybersecurity property insurance has the characteristics of the cybersecurity industry. As a new cybersecurity product, cybersecurity insurance plays an important role in protecting enterprises against risks, such as data loss and network interruption, so cybersecurity property insurance may be regarded as a novel comprehensive product for cybersecurity in a broad sense. To sum up, the premiums of cybersecurity property insurance increase accordingly when the revenues of the cybersecurity industry increase, and vice versa.

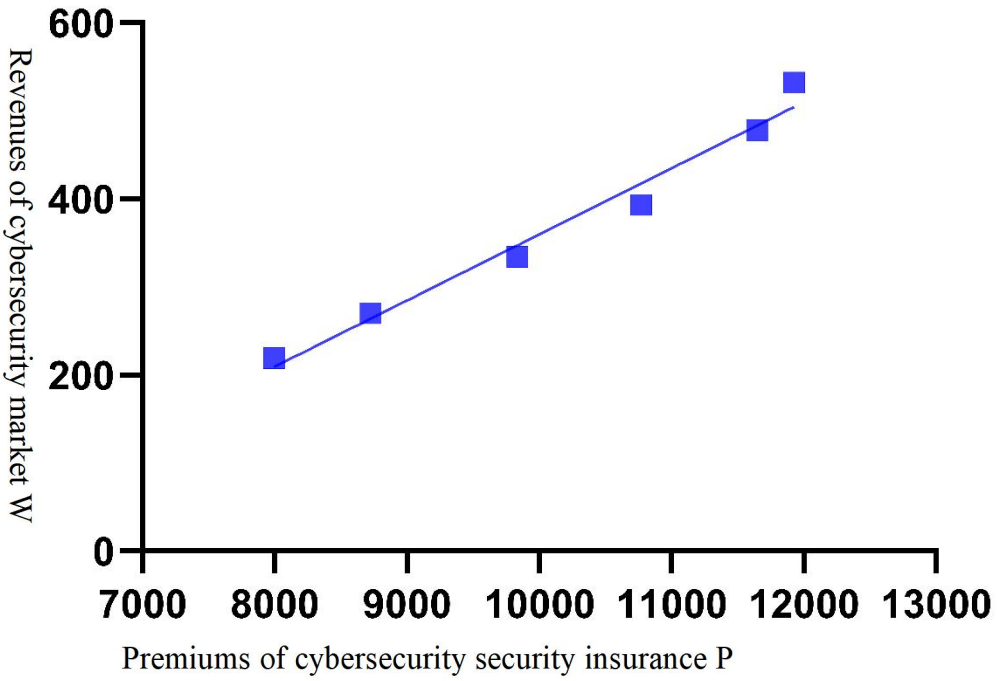


Figure 10. Relationship between premiums of cybersecurity property insurance and revenues of the cybersecurity industry

To sum up, enterprises can get services, such as loss control, claim, and statistical analysis, from insurance companies by purchasing cybersecurity property insurance with small fixed premiums every year. On the one hand, they can reduce losses caused by cybersecurity threats, such as unavailability of information equipment, business interruption and information leakage, and reduce the cost of handling cybersecurity incidents and improve post-disaster recovery capabilities. On the one hand, the increasing demand for enterprise cybersecurity property insurance will drive the market demand for cybersecurity vendors, and then drive the revenues of insurance business.

5) Regression Analysis

Though the small sample size of statistics (only data from 2015 to 2020) may bias the results of regression analysis, this paper provides examples suggesting relevant ideas and

processes of linear regression and analyzes and predicts the relationship between variables in the model to inform future research when sufficient statistics become available. In this paper, Graphpad Prism 9.4.1 is used with the data in Table 3 for regression analysis with Model (1), as shown below.

(1) Descriptive statistics

From the descriptive statistics (shown in Table 4), the average values of variables -- revenues of the cybersecurity market (W), demand for enterprise cybersecurity property insurance (Q), and enterprise cyber risk losses (S) -- are slightly larger than the medians, and the standard deviations are relatively large. This indicates that the data are scattered wide and the sample data are mainly concentrated on the smaller side.

Table 4. Descriptive Statistics

	Observations	Average	Median	Standard deviation	Variance	Minimum value	Maximum value
P	6	10150.41	10302.63	1585.79	2514731	7994.97	11928.58
W	6	3710	3635	1204.392	1450560	2190	5320
Q	6	14821.86	14473.6	1653.768	2734948	13419.19	18060.41
S	6	1868.672	1708.975	773.5613	598397.1	900.06	2911.76

(2) ANOVA

Analysis of variance (ANOVA) is used to test the significance of the difference between the means of two or more samples. It is done by analyzing the contribution of variations from different sources to the total variance to determine the significance of controllable variables with respect to the results of research.

Table 5 gives the results of variance analysis in regression fitting. Sig is the

probability when F value is greater than F critical value. From the model, the significance probability is less than 0.05, and all the original hypotheses with regression coefficients being 0 are rejected. It is also possible to see that the regression sum of squares is 1.254E+7, and the residual sum of squares is 3.142E+4 with a total of 1.257E+7. The regression sum of squares accounts for the most total sum of squares, which suggests that the linear model explains the most total sum of squares, and the model has good fitting.

Table 5. ANOVA Results

ANVOA[a]						
Model		Sum of squares	Degree of freedom	Mean square	F	Significance
1	Regression	12542237.232	3	4180745.744	266.150	.004[b]
	Residual error	31416.515	2	15708.258		
	Total	12573653.748	5			

a. Dependent variable: P

b. Predictive variables: (constant), S, Q, W

(3) Significance analysis

The P value is used to test the significance of regression equation coefficients. Generally, $P < 0.001$ indicates extremely high significance; $0.001 < P < 0.01$ indicates high significance; $0.01 < P < 0.05$ indicates significance; $P > 0.05$ indicates low significance. From Table 4, the P value of demand for cybersecurity property insurance Q and enterprise network risk loss S is greater than 0.05, which indicates that independent variables Q and S have no significant impact on the model, possibly because of insufficient statistical data or multicollinearity.

Table 6. Significance analysis of regression coefficients

Parameter estimates	Variable	Estimate	Standard error	95% CI (asymptotic)	|t|	P value	P value summary
β0	Intercept	6638	666.8	3769 to 9508	9.955	P=0.0037	*
β1	W	1.998	0.3621	0.4403 to 3.556	5.519	P=0.0313	*
β2	Q	-0.1512	0.04477	-0.3439 to 0.04140	3.378	P=0.0776	ns
β3	S	-0.8882	0.5735	-3.356 to 1.579	1.549	P=0.2616	ns

(4) Residual normality test

Prerequisites of an ideal regression model: 1) There is no serial correlation between stochastic error terms; 2) random error items follow a normal distribution; 3) the variance of random error items is the same or fixed constants. A residual error is the difference between the sample value and the value on the regression line (also called regression fitting value). The residual error test checks whether the residual error obtained after regression fitting meets the above three criteria. The Shapiro-Wilk test verifies whether the data of a random sample comes from the normal distribution, and the Kolmogorov-Smirnov test (K-S test), based on a cumulative distribution function, checks whether there is a significant difference from the normal distribution. From Table 7, the Shapiro-Wilk test value is 0.9657, and the P value is 0.86, significantly greater than 0.05, so the conformity to the normal distribution is rejected. The Kolmogorov-Smirnov value is 0.18, and the P value > 0.1, so the sample values are considered to follow a normal distribution.

Table 7. Residual Normality Test

Normality of Residuals	Statistics	P value	Passed normality test (alpha=0.05)?	P value summary
D'Agostino-Pearson omnibus (K2)	N too small			
Anderson-Darling (A2*)	N too small			
Shapiro-Wilk (W)	0.9657	0.8621	Yes	ns
Kolmogorov-Smirnov (distance)	0.1767	>0.1000	Yes	ns

In addition, the Q-Q plot can be used to identify whether the sample data approximates a normal distribution. If the points on the Q-Q plot are approximately near a straight line, the sample data follows the normal distribution. The consistency between the observed value and the expected value of P value is compared. From Figure 11, the data points are generally located on the diagonal, indicating that the two sets of values are basically the same. That is, the two samples have good repeatability.

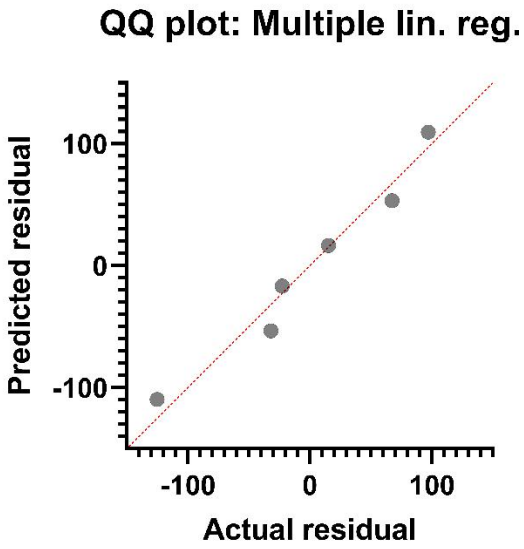


Figure 11. Q-Q Plot

To sum up, the regression model's results may be biased due to the insufficient sample size of statistics. Nevertheless, the results from the variance analysis and significance analysis show that the regression equation in general and the coefficients are significant, so the following regression equation can be obtained:

$$P = 1.998W - 0.151Q - 0.882S + 6638$$

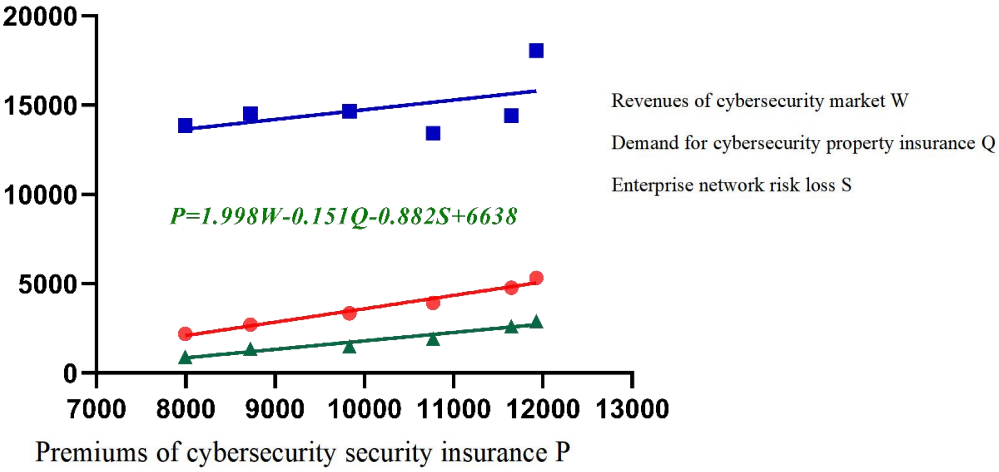


Figure 12. Regression Analysis Trend Chart

The modeling above has analyzed the relationship between premiums of cybersecurity property insurance, revenues of the cybersecurity market, demand for enterprise cybersecurity property insurance, and enterprise cyber risk losses. The deficiencies in the modeling are also accounted for. As for the expansion of cybersecurity property insurance market, enterprise managers need some time for pondering before deciding to purchase cybersecurity property insurance. On the one hand, they would consider the relationship between their vulnerabilities and investment in comprehensively and their information security risks, the reputation of insurance companies, etc.; On the other hand, they would the possibility of adverse selection to the advantage of insurance companies due to information asymmetry related to cybersecurity. Whether the time of decision-making allows lead time or cause lag time cannot be effectively verified due to the lack of empirical data at present. This will be studied with the Granger causality test the data sample becomes sufficient.

4.4 Case Studies Of Cybersecurity Property Insurance

Cybersecurity has been a concern ever since the birth of networks. In the Internet era, networks have extended to every corner of our communities. Countries, communities,

organizations and individuals are inseparable from the networks. Cybersecurity risks exist everywhere, and cybersecurity incidents happen frequently.

Case 1: In August 2019, a data leak accident occurred in Binance, the world's biggest cryptocurrency exchange. Hundreds of users' Know Your Customer (KYC) images were seen on the Internet, and tens of thousands of users may be affected in the future. After obtaining the information, the hackers allegedly threatened the exchange to pay 300 bitcoins or they would make public all KYC images in their hands. Evidence shows that the leaked images may have been used to change account information and set up fraudulent accounts. Binance said it would offer lifetime VIP membership to all affected users.

Coincidentally, Binance also suffered a large-scale system attack two months ago and lose a large number of user API keys, Google authentication 2FA codes and other related information. Hacker groups used complex techniques, including phishing, viruses and other attacks. In this incident, a total of 7,000 bitcoins were stolen by hackers. According to an official statement, Binance will use the "SAFU Fund" to cover all the losses from the attack and no users will have any loss.

Case Study 2: Colonial Pipeline is the largest refined products pipeline in the United States, transporting more than 100 million gallons of fuel daily. On May 7, 2021 (EST of U.S.), Colonial Pipeline was attacked by ransomware. As a result, the oil pipeline operations in the eastern coastal states of the United States were halted, and the White House declared a state of emergency. It was not until May 12 when Colonial Pipeline announced the gradual resumption of fuel transportation.

In terms of losses, the main losses in this case were related to the ransom payment,

business interruption and indemnification in third-party collective litigations. Among them, Colonial Pipeline paid about USD 4.4 million for the ransom, of which USD 2.3 million were recovered, so the net loss caused by the ransom was about USD 2.1 million US; the business interruption led to net profit loss of nearly USD 9 million per week to the company according to the calculation of Reuters based on the U.K.; in third-party collective litigations, the third-party claims exceed USD 5 million.

According to public information, Colonial Pipeline insured its assets, such as networks and data with Beazley and other insurance companies, with policy limits of at least USD 15 million. The clauses of policies currently sold by Beazley show that the policies cover computer forensics traceability, public relations activities for incidents, loss estimation and other expenses, business interruption losses, subordinate business interruption losses, losses caused by network ransom, data recovery costs, etc. The ransomware attack on Colonier Company was a typical incident of cyber insurance, and the ransom payment, business interruption, and other known losses may trigger claims under the policies.

Compared with open compensation cases in other countries, few cases were reported in China, and enterprises would avoid confirming such information for the sake of brand image.

Case Study 3: A Chinese medical institution deployed a large number of security equipment and met the requirements for protection of the specified class. One day, the medical institution received a notice from a group of hackers, who claimed that they have controlled the medical institution's core business systems and demanded a ransom of RMB 250,000. If their demand was not met, they would sell the patient's electronic medical records and personal information on the black market or release them on the Internet, which would cause extremely adverse social impact.

After the incident, the medical institution activated a dual-channel reporting mechanism by informing both the insurance company and a security company. Upon receipt of notification, the two companies quickly set up a joint investigation team and assign an emergency response manager to the scene and coordinate the work of security technical experts, legal advisers, and public relations, emergency response and other personnel in handling the incident. After several rounds of negotiations, the insurance company paid RMB 200,000 for data recovery. At the same time, the medical institution restored important data and systems and completed further system security reinforcement with the assistance of security experts from the security company. The impact of the incident was minimized with further guidance and assistance from public relations personnel and legal advisors. The expenses for data recovery and public relations activities involved in the incident were paid by the insurance company, which provided strong support for the client's undisrupted operation and effectively recovered their reputation and economic losses.

1) Lessons from the case studies for enterprises

Traditionally, the application of cybersecurity technology had been thought to be able to control cyber risks gradually. However, key infrastructures are stilled attacked via networks, even if security efforts have been made according to the requirements for protection by cybersecurity classes in China, and in countries like the United States, which have highly developed in cybersecurity technology. This reflects the uncertainty in cybersecurity. The application of cybersecurity defense products may reduce the frequency of network incidents, but it cannot totally eliminate their possibility, let alone reducing the huge losses brought by them.

Moreover, the case studies above also show that even residual cyber risks may cause business instability and large financial losses of the affected organizations. As insurance

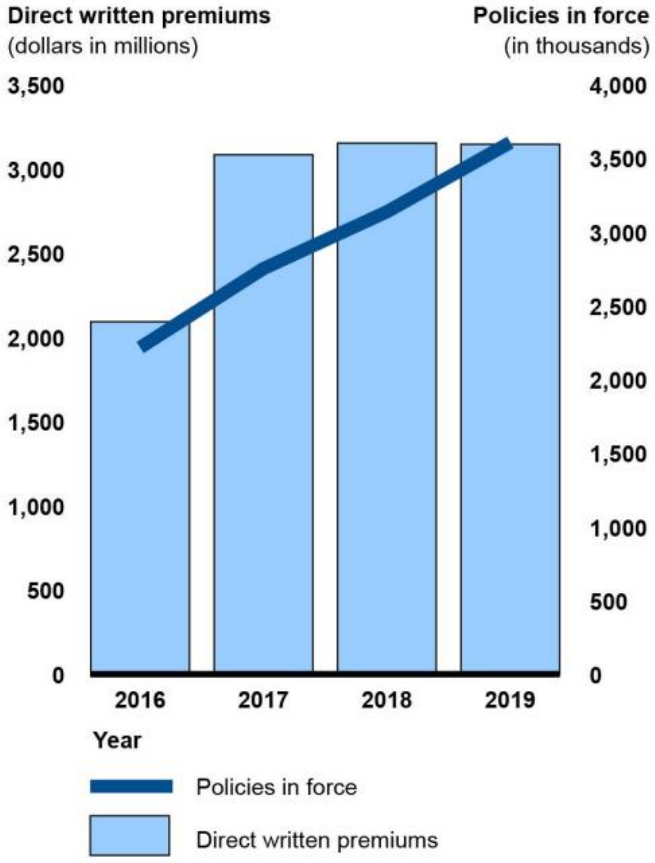
provides compensation in the case of loss and economic leverage, enterprise can improve their ability of hedging and post-disaster recovery ability by having their data assets covered by cybersecurity property insurance and paying relatively small amounts of premiums. Therefore, enterprises can get standardized security products and services by purchasing cybersecurity property insurance with small fixed premiums every year. In this way, they can reduce losses caused by cybersecurity threats, such as unavailability of information equipment, business interruption and information leakage, and reduce the cost of handling cybersecurity incidents and improve post-disaster recovery capabilities.

Finally, the case studies above highlight the severe losses caused by cybersecurity threats, which send alarms to high-risk enterprises that have not purchased cybersecurity property insurance, and indirectly prove the importance of cybersecurity property insurance. The case studies also show that enterprises that have purchased cybersecurity property insurance can not only make up for direct economic losses such as terminals, data leakage and emergency response expenses with the compensation from insurance companies, but also receive professional and standard security services and timely guidance for emergency response to reduce indirect losses, such as company reputation. Therefore, the refining of functions of cybersecurity property insurance, provision of more targeted services by insurance technology companies, and availability of more abundant case studies of cybersecurity property insurance attract more high-risk enterprises to purchase cybersecurity property insurance and facilitate the promotion of cybersecurity property insurance.

2) Impact of Incidents on the Insurance Market

On the one hand, the frequent occurrence of cybersecurity incidents drives the acceptance of and demand for cybersecurity property insurance in the market. According to the report "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving

Market" released by the United States Government Accountability Office in 2021[12], first, the growing frequency and severity of cyber attacks have led more insurance clients to opt for cyber coverage—up from 26% in 2016 to 47% in 2020. Second, the demand for cyber insurance has increased. According to the analysis of data from S&P Market Intelligence and NAIC, the number of cybersecurity policies that came into effect from 2016 to 2019 increased from 2.2 million to more than 3.6 million, an increase of about 60%; the total written premiums increased from USD 2.1 billion to USD 3.1 billion, an increase of by 50% (See Figure 12). The report also noted that the two major drivers for the growth of cyber insurance are suffering cyber attacks and hearing of losses due to cyber attacks suffered by other enterprises.



[12] Source: https://www.gao.gov/assets/720/714429.pdf

Figure 13. Changes in Written Premiums and Number of Policies of Cyber Insurance from 2016 to 2019[13]

On the other hand, frequent incidents have led to increase in cybersecurity increase premiums and decrease in coverage limits. Data show that cyber insurance premiums remained relatively stable in 2017 and 2018, and increased significantly in 2020. From the third to the fourth quarter of 2020, the cyber insurance premiums paid by clients increased by 10% to 30%, as shown in Figure 13. The reasons include the increase in client demand and more frequent and serious cyber attacks having caused increased losses for insurance companies, especially those due to ransomware attacks. In addition, the continually increasing frequency and severity of cyber attacks, especially ransomware attacks, have led insurers to reduce cyber coverage limits for certain riskier industry sectors, such as health care and education, and for public entities and to add specific limits on ransomware coverage.

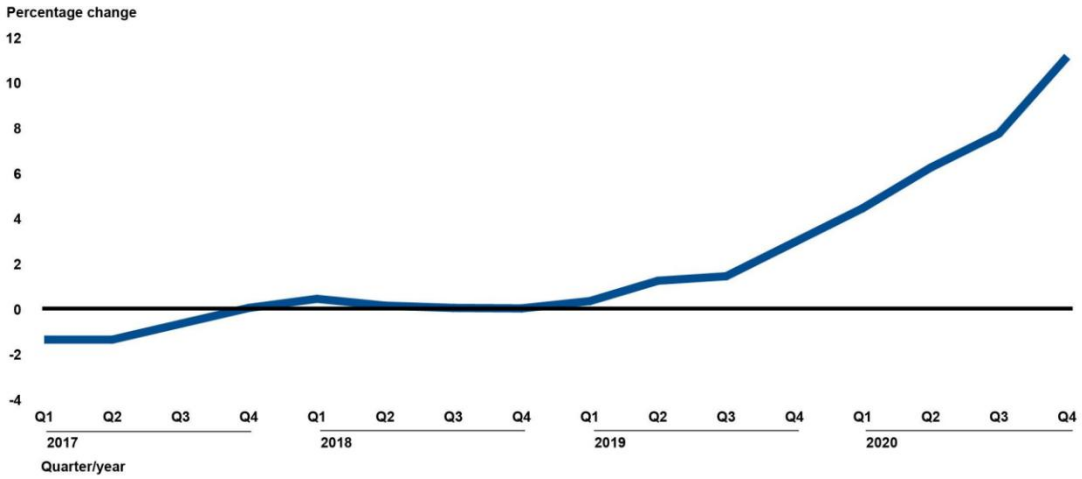


Figure 14. Change in Cyber Insurance Premiums, 2017–2020[14]

[13] Source: S&P Market Intelligence, NAIC, GAO
[14] Source: GAO presentation of data from Council of lnsurance Agents & Brokers.

5. RECOMMENDATIONS ON MEASURES FOR DEVELOPING CYBERSECURITY PROPERTY INSURANCE

1) Gradually Harmonize Metrics Of Industrial Statistics

A range of harmonized metrics of industrial statistics facilitates scientific and objective measurement of the development of the cybersecurity industry. Currently, only the China Academy of Information and Communication Technology and the China Cybersecurity Industry Alliance release collect data on the cybersecurity industry's size every year. However, they have not disclosed their respective metrics of statistics and made changes to the same since 2020. The changes between the old and new metrics were also unknown. The government or industry associations should clearly define the cybersecurity industry's scope and harmonize metrics of statistics of the industry considering the fact that both the upstream vendors of hardware and downstream vendors of applications of the cybersecurity industry live together with other industries. On this basis, it is possible to scientifically estimate various statistics of the cybersecurity industry, such as industrial output value, import and export value, and the people working in the industry, to provide scientific quantitative information for driving the industry's development and policy making.

2) Strengthen Disclosure Of Information On Network And Information Security Incidents And Actively Develop Basic Databases Of Cybersecurity

In this paper, the analysis of the production model suggests that the results on the cybersecurity property insurance market's size are based due to the lack of essential data on revenues of the cybersecurity market, demand for enterprise cybersecurity property insurance, and enterprise cyber risk losses. As for the development of cybersecurity property insurance, the lack of sufficient essential data hinders insurers from developing products and pricing products, while the insured are prone to make poor decisions on buying insurance without

sufficient and comprehensive information. Therefore, it is necessary to legislate for mandatory disclosure of information on cybersecurity incidents to drive the perfection and expansion of the basic databases, effectively protect data, and improve data availability. Insurers will be able to develop products and offer more satisfactory insurance plans based on relevant data, and the insured will be able to analyze risks before purchasing products. Therefore, three recommendations are given to improve the credibility and reliability of data: first, legislate for disclosure of information on cybersecurity incidents to ensure the credibility and reliability of data in the databases with public authority; second, establish a cybersecurity intelligence network to broaden data sources, consolidate data from different sources and share security situation awareness; third, create mechanisms to ensure security and confidentiality obligations and set up professional institutions to collect data on cybersecurity incidents anonymously.

3)Facilitate The Development Of The Cybersecurity Property Insurance Regulation System

Adequate regulations on cybersecurity property insurance are required to provide the legal basis for development policies, handling possible disputes, and protecting the legitimate rights and interests of the insured. Without adequate regulations, enterprises are likely to question the real benefits of cybersecurity property insurance. In such cases, it would be difficult for them to make the right decisions even if they become aware of risks accurately. To improve the benefits of cybersecurity property insurance, two recommendations are given. First, improve the legal environment for cybersecurity property insurance. China should classify and summarize network and information assets and define a complete hierarchy to provide a legal basis for policy development. The body of laws, judicial interpretations, regulations, regulatory documents, departmental rules, and related documents as well as local

laws and regulations, and related legal systems should address the differences between cybersecurity property insurance and insurance in general. Second, strengthen the regulatory role of the China Banking and Insurance Regulatory Commission (CBIRC) to urge relevant institutions to comply with ethics, laws, and regulations in the storage and application of collected information. Companies are advised to establish independent cybersecurity insurance supervision organizations as cybersecurity insurance supervision requires specialized expertise in network and information technology.

6. SUMMARY AND FOLLOW-UP RESEARCH

The concept of network and information security has gradually entered the era of "active security" from "passive defense" along with the continuous digital transformation in various industries and fields. This paper has discussed the feasibility and necessity of combining cyber insurance with commercial property insurance to form cybersecurity property insurance based on the status quo of commercial property insurance and cyber insurance.

Feasibility: First, the new-type information infrastructure has gradually become a new driver of economic growth, leading to frequent occurrence of incidents and an expanding cybersecurity market, which has provided favorable market conditions for the development of cybersecurity property insurance. Second, the adoption of laws and regulations related to cybersecurity have further clarified the rights and obligations of all players involved in cyberspace, which has provided the legal and institutional conditions for the development of cybersecurity property insurance; cybersecurity property insurance will also play a fundamental role in cybersecurity and help realize the overall security required in the Cybersecurity Law. Finally, risk management and technical service institutions, such as cybersecurity companies and insurance technology companies, actively leverage their specialized advantages in actively exploring products and service solutions of cybersecurity-related insurance, and deeply participating in the industry ecosystem of cyber insurance, which has provided a system environment for the development of cybersecurity property insurance.

Necessity: First, as cyber insurance appeared late in China, most enterprise clients know little about cyber insurance and are unlikely to accept transferring cyber risks through insurance. This results in lack of motivation to purchase cyber insurance, while the market of

commercial property insurance is large, and insurance companies have rich experience in promoting commercial property insurance. Combining these two categories could promote the expansion of cyber insurance through the scale effect of commercial property insurance. Second, in the context of digital transformation, commercial property insurance cannot meet the needs for risk transfer for new-type assets, but cyber insurance provides the means of risk transfer for networks, data and other assets. Combination of the two categories will expand the coverage of liabilities to increase products' competitiveness and meet the needs of enterprises. Finally, China's commercial insurance premiums have declined and cybersecurity threats faced by enterprises are gradually increasing since the outbreak of the COVID-19 pandemic in 2020. Therefore, the combination of cyber insurance and commercial property insurance as cybersecurity property insurance not only responds to the requirement for innovation of insurance services, but also meets the needs of enterprises for transfer of cyber risk, providing more comprehensive high-quality protection for the production and operation of enterprises in the post-COVID period.

This paper obtains the following findings through hypothetical models: Enterprises can get services, such as loss control, claim, and statistical analysis, from insurance companies by purchasing cybersecurity property insurance with small fixed premiums every year. On the one hand, they can reduce losses caused by cybersecurity threats, such as unavailability of information equipment, business interruption and information leakage, and reduce the cost of handling cybersecurity incidents and improve post-disaster recovery capabilities. On the one hand, the increasing demand for enterprise cybersecurity property insurance will drive the market demand for cybersecurity vendors, and then drive the revenues of insurance business.

In this last section, recommendations are given on measures for developing

cybersecurity property insurance. First, gradually harmonize metrics of industrial statistics to provide scientific quantitative information for driving the industry's development and policy making. Second, strengthen disclosure of information on network and information security incidents and actively develop basic databases of cybersecurity so insurers will be able to develop products and offer more satisfactory insurance plans based on relevant data and the insured will be able to analyze risks before purchasing products. Third, facilitate the development of the cybersecurity property insurance regulation system to improve the benefits of cybersecurity property insurance.

Deficiencies exist in the study presented in this paper due to the constraints of time, data availability, and other factors. To address these deficiencies, the following improvements are expected in the follow-up research: First, the demand for enterprise cybersecurity property insurance and enterprise cyber risk losses are represented by relevant data, which are also in dearth. The government and insurance industry are expected to establish relevant databases, so future research can rely on indemnification data to study cyber risk losses. Second, the empirical analysis of the correlation between the influencing factors of cybersecurity property insurance is insufficient due to the limited sample data. More detailed studies on the relationship between variables would be possible when sufficient data become available later. Third, this paper has explored the feasibility and necessity of cybersecurity property insurance by combining cyber insurance with enterprise property insurance. Later studies may cover the terms and pricing models of cybersecurity property insurance.

REFERENCES

[1] Xu W.. Connotation and Development of Cyber Insurance [J]. Shanghai Insurance Monthly. 2022, (01): 23-25.

[2] Che Y.. A Study on Development of Network Information Security Insurance in China --- An Example of Cooperation between Zhongan Insurance and DAS-Security [D], Liaoning University, 2020.

[3] Gao L., Yang A.. Latest Development of Network Insurance in Europe and the US and Inspirations for China [J]. Insurance Studies. 2010, (11): 75-80.

[4] Liang N., Zhang K., Song L.. Analysis and Recommendation on Development of Cybersecurity Comprehensive Insurance [J]. Financial Technology Time, 2017 (12): 92-94.

[5] Tang J., Li Y.. On Improvement of Network Insurance Market Supervision [J]. Zhe Jiang Finance. 2014, (06): 73-79.

[6] Wang Y.. A Study and Design of Information Security Insurance Underwriting System [J]. Insurance Studies. 2008, (06): 72-75.

[7] Gao L., Lv W.. On Establishment of Network Information Security Insurance System in China [J], Insurance Studies, 2011, (7): 86-91.

[8] Liu C., Gao J.. Feasibility Analysis of Win-Win Interaction Between Information Security Industry and Insurance Sector [J]. Documentation, Information & Knowledge, 2002 (01): 41-44.

[9] Jiang J.. On Development of Network Information Security Insurance in China [J]. Information Systems. 2003, 26 (4): 356-359.

[10] Wang Y.. A Study on Emerging Development and Regulation of Cyber Insurance [J]. China Information Security, 2017 (03): 45-47.

[11] Wang X., Wang Y.. Strategic Analysis of Cyber Insurance --- Research Architecture Based on Life Cycle of Cyber Insurance [J]. Journal of Intelligence. 2017, 36 (11): 34-40.

[12] Tang J., Mo C.. A Study on Innovation and Development of Cyber Insurance in Digital Economy Era [J], Southwest Finance. 2022, (01): 52-64.

[13] Gu J., Mei S., Zhong W.. Incentive Mechanism for Investment in Information System Security Based on Cyber Insurance [J]. System Engineering --- Theory and Practice.

2015, 35 (4): 1057-1062.

[14] Yang Y., Wang Y.. A Study on Optimal Cyber Insurance Contract Model under Moral Risks [J]. Chinese High Technology Letters. 2016, 26 (8): 732-738.

[15] Yuan S.. An Empirical Study on Factors Influencing Cyber Insurance and Cyber Risk Perception [D], Hunan University. 2018.

[16] Dong K., Xie Z., Zhen J., Hong Z.. A Study on Network Information Security Risk Measurement and Insurability Based on Data Breach Types [J]. Insurance Studies. 2019, (11): 25-41.

[17] Dong K., Xie Z., Zhen J.. Optimal Decision Analysis of Enterprise Information Security Investment and Network Insurance under Mandatory Constraints [J]. China Journal of Management Science. 2021, 29 (6): 70-81.

[18] Wang X.. Roadmap of Cyber Insurance Law and Policy [J]. Journal of Political Science and Law, 2011, 28 (01): 15-21.

[19] Wang T.. A Comparative Study on Information Security Liability Insurance System [J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 2018, 30 (03): 60-8.

[20] Fang G., Chu B.. A Study on Legal Governance of Maritime Cyber Risk Insurance [J]. Jiangxi Social Sciences. 2020, 40 (05): 179-191.

[21] Zhang R., Wu Y.. A Study on Building of Personal Information Security Liability Insurance System [J]. Journal of Regional Finance Research. 2021, (05): 52-60.

[22] Wang C.. A Study on Pricing of Against Bitcoin Ransomware Invasion --- Against Market Background of Malicious Control of Important Personal Information of College Students [C]. 2017 China International Conference on Insurance and Risk Management, 2017.

[23] Zhao F.. A Study on Network Information Security Insurance and Its Pricing [D]. Southwestern University of Finance and Economics, 2019.

[24] Chen W., Lu K., Chen M., et al. Insurance Customization and Marketing Model of Network Personal Information Security [J]. China Market. 2020, (03): 186-188.

[25] Ma Z.. A Study on Cyber Insurance Pricing Model under Scale-free Network --- Taking Monte Carlo Simulation as Example [D]. Nankai University, 2020.

[26] Wei H., Lin B.. Insurance (3rd Edition) [M]. Beijing: Higher Education Press, 1999, 110-111.

[27] Huang H.. Ideas and Trends of Reform of Major Property Insurance Categories in China [J]. Shanghai Finance, 1994 (02): 36-37.

[28] Gao J., Yin L.. Discussions on Changing the Underwriting of Commercial Property Insurance [J]. Insurance Studies, 1999 (07): 13-16.

[29] Shi W.. Maintaining Property Insurance is the Fundamental Approach of Enterprises in Prevention of and Response to Disasters [J]. Insurance Studies, 1999 (04): 6-7 +23.

[30] Chen B.. Risk Management and Insurance (2nd Edition) [M]. Beijing: Tsinghua University Press, 2005, 147-157.

[31] Su Y.. On Development of Property Insurance for Private Enterprises in China [J]. Insurance Studies, 2007 (03): 21-22 +25.

[32] Zhu M., Kui C.. Demand Analysis of Commercial Property Insurance in China [J]. China Insurance, 2009 (8): 20-23.

[33] Yan W., Su B.. Discussions on Commercial Property Insurance Management [J]. Theory Journal, 2012 (S1): 77.

[34] Zou, H., Adams, M.B., Buckle, M.J.. Corporate Risks and Property Insurance: Evidence from the People's Republic of China [J]. Journal of Risk and Insurance. 2003, 70(2):289-314.

[35] Zou, H., Adams, M.B.. The corporate purchase of property insurance: Chinese evidence [J]. Journal of Financial Intermediation. 2006, 15(2):165-196.

[36] Zou, H., Adams, M.B.. Corporate Insurance and Debt: The Case of China [J]. Journal of Applied Corporate Finance. 2009; 21(1):87-89.

[37] Song L.. Factor Analysis of Commercial Property Insurance Premiums [J]. China Insurance, 2008 (08): 56-58.

[38] Zhu M., Lu Y., Kui C.. Analysis of Factors Influencing Demand for Commercial Property Insurance in China --- An Empirical Study Based on Regional Panel Data [J]. Journal of Financial Research, 2010 (12): 67-79.

[39] Zhao H., Su H.. A Study on Factors Influencing Demand for Property Insurance in China --- Panel Data Based on Region Weight and Time Weight [J]. Insurance Studies, 2013 (02): 38-44.

[40] Huang F., Zhang M.. Premium marketization and Demand for Commercial Property Insurance [J]. Journal of Financial Research, 2014 (12): 164-177.

[41] Yang Y., Zhong Y., Lu L.. A Study on Issues Related to Commercial Property Insurance

Behavior [J]. Commercial Times, 2010 (32): 89-91.

[42] Yang B., Yu R., Ou H.. Institutional Environment, Transaction Cost and Insurance Demand of Listed Companies [J]. Journal of Nanjing University (Philosophy, Humanities and Social Sciences), 2010, 47 (05): 27-36.

[43] Xiao J., Liu M., Hong R.. A Study on Demand for Property Insurance of Export-Dependent Enterprises --- Empirical Evidence from Chinese Manufacturing Enterprises [J]. Management Review, 2021, 33 (06): 65-75.

[44] Zhao H., Su H.. A Study on Factors Influencing Demand for Property Insurance in China --- Panel Data Based on Region Weight and Time Weight [J]. Insurance Studies, 2013 (02): 38-44.

[45] Ju L., Xue C., Zhao T., Cong Y.. Macroeconomic Policy Expectation and Insurance Demand [J]. Consumer Economics, 2021, 37 (01): 27-38.

[46] Liu Y.. Application of Financial Feasibility Analysis in Mergers and Acquisitions ---Based on Enterprise Value Evaluation [J]. Communication of Finance and Accounting, 2017 (11): 11-14.

[47] Zhang M.. Challenges and Regulatory Responses to Development of Cyber Insurance [J]. Shanghai Insurance Monthly, 2022 (02): 12-15.

[48] Philpot J.. Digital SME Input to the Consultation on the Proposal for a Revised Directive on Security of Network and Information Systems (NIS2 Directive) [R]. European Digital SME Alliance, Brussels, 2021.

[49] Lu M., Wang T.. Digital Management and Factor Marketization: Study of Basic Theories and Innovation of Digital Assets [J]. South China Finance, 2020 (08): 3-12.

[50] Lu M.. Study of Development Strategy of Digital Microfinance of Commercial Banks in Context of COVID-19 --- Based on Development Perspective of Future Banks [J]. Journal of Xinjiang Normal University (Philosophy and Social Sciences), 2020, 41 (06): 28-42.

[51] Lu M., Zhou J.. Small and Medium-Sized Commercial Banks: Risk Management, Corporate Governance and Reform Strategy [J]. Journal of University of Jinan (Social Science Edition), 2020, 30 (04): 100-113 +159.

[52] Eling M., Schnell W.. Ten key questions on cyber risk and cyber risk insurance [J]. The Geneva Association-‘International Association for the Study of Insurance Economics’, 2016.

[53] Kshetri N.. The global cybercrime industry: economic, institutional and strategic perspectives [M]. Springer Science & Business Media, 2010.

[54] Yan Y., Du J.. Impact and Lessons of COVID-19 on Insurance Sector [J]. Economic and Trade Update, 2020 (20): 100-101.

[55] Wang Y., Zhang D., Wang X., Fu Q.. How Does COVID-19 Affect China's Insurance Market? [J]. Emerging Markets Finance and Trade. 2020, 56(10):2350-2362.

[56] Chu M., Dang Y.. A Study on Impact of COVID-19 on International Market Cycle of Property Insurance and Reinsurance [J]. Insurance Studies, 2021 (04): 3-23.

[57] Li Z., Cheng J.. Impact of COVID-19 on Chinese Insurance Sector and Development Recommendations [J]. Marketing Circles, 2020 (38): 41-43.