Global Economic Perspectives Vol 1 Issue 3 2023

Original Research Article

Open Access

Omniscient Pte.Ltd.

Development Opportunities, Challenges, and Strategies for Cybersecurity Insurance in the Digital Economy Era

Yi-Chen Guo*

University College London, London, 999020, United Kingdom

***Correspondence to:** Yi-Chen Guo, University College London, London, 999020, United Kingdom,
E-mail: 1322600981@qq.com

Abstract: This paper proposes that in the current development of cybersecurity insurance in the digital economy era, there are opportunities such as increasing emphasis on cybersecurity, development of cybersecurity insurance technology, and continuous expansion of the cybersecurity industry. However, some enterprises face challenges such as the lack of industry standards, difficulty in defining data assets, and challenges in securing cybersecurity data, which hinder the development of cybersecurity insurance. This paper suggests that in order to promote the vigorous development of cybersecurity insurance in the digital economy era, strategies such as increasing government regulatory efforts, strengthening management of insurance companies, and enhancing cybersecurity protocol management should be adopted to better address the risks inherent in cybersecurity insurance and promote the vigorous development of China's digital economy.

Keywords: digital economy era; cybersecurity insurance; development opportunities; challenges; strategies

Introduction

With the accelerated pace of development and the expanding scope of application in the digital economy, cybersecurity issues related to digital technologies have gradually entered the public's view. Ensuring the confidentiality and integrity of enterprise data, defending against unlawful cyber intrusions, and maximizing the effectiveness of cybersecurity insurance applications have become key issues that enterprises need to focus on.

1. Development Opportunities for Cybersecurity Insurance in the Digital Economy Era

1.1 Increasing Emphasis on Network Security

Since the 18th National Congress of the Communist Party of China, our country has taken many measures to maintain network security. The relevant policy and regulatory system is continuously improving, the operation mechanism of network security is becoming more perfect, and the capabilities in protecting key information infrastructure, managing data security, and protecting personal information are continuously strengthening. This has achieved remarkable

results. For example, during this period, China has promulgated a series of laws and regulations to safeguard network security, such as the Cybersecurity Law, the Personal Information Protection Law, the Data Security Law, and the Measures for Cybersecurity Review, aiming to gradually improve China's network security management system, promote the systematic, authoritative, and comprehensive management of digital networks, and effectively enhance the security of China's network environment. Additionally, China has also implemented the "National Anti-Fraud" app, which, when installed on smartphones, can help the public effectively prevent behaviors such as network fraud and safeguard their property security. This demonstrates the high degree of attention the country pays to network security. It conveys a correct concept of network security to the public, and with the country setting an example, people and enterprises will inevitably pay more attention to network security issues. As a result, the market for cybersecurity insurance will vigorously develop, providing a broader space for individuals and enterprises engaged in network security construction.

1.2 Development of Cybersecurity Insurance Technology

Under the trend of economic globalization, the digital economy has experienced robust growth. Many domestic and international enterprises have been strengthening their internal digitalization efforts in recent years, aiming to construct a comprehensive, efficient, automated, and modernized system to keep pace with the development trends of the times. In this process, cybersecurity insurance technology, as an integral component of digital technologies, naturally has significant room for development.For instance, during the 2022 World Artificial Intelligence Conference Security Summit, the "2022 Cybersecurity Insurance Technology White Paper" was officially released, which introduced the cybersecurity insurance technology model for the first time and outlined the application of data science in new cybersecurity insurance. Prior to this, the concept of "cybersecurity insurance technology" was not clearly defined domestically or internationally. The appearance of the white paper filled this gap and laid a solid theoretical foundation for the development, innovation, and transformation of the cybersecurity insurance field. In the future, China's cybersecurity insurance industry, machine-derived businesses, and products will be driven by this development, gaining broader opportunities for growth.This demonstrates that the development of cybersecurity insurance technology is an inevitable trend in the era of the digital economy. Enterprises should seize this opportunity, ride the wave of the times and policies, and swiftly capture market share.

1.3 Continuous Expansion of the Cybersecurity Industry

The continuous expansion of China's cybersecurity industry can be observed in several aspects:(1). Establishment of Public Big Data National Key Laboratories: Currently, many provinces in China have established public big data national key laboratories. These laboratories aim to conduct research on the integration, integration, security, privacy protection, block data, regional governance, and other aspects of public big data, in order to promote the continuous improvement of China's network security technology level through scientific research results.(2). Development of Cybersecurity-related Industries: Presently, over 500 universities and colleges in China offer majors related to network information security. Moreover, the industry related to network security technology is expected to reach nearly 217 billion yuan in 2022, representing a year-on-year growth of 13.9%. All of the above are manifestations of the continuous expansion of the cybersecurity industry.

2. Difficulties in the Development of Cybersecurity Insurance in the Digital Economy Era

2.1 Lack of Well-defined Industry Standards

For any industry, well-defined industry standards are crucial for promoting standardized development. However, the cybersecurity insurance industry has not been around for long, and industry standards have not yet been well-established. As a result, many enterprises find themselves in a trial-and-error situation, making it easy to fall into pitfalls or be overwhelmed by difficulties during the development process. Several reasons contribute to the lack of well-defined industry standards in the cybersecurity insurance industry:

Limited Historical Data: Compared to other types of insurance such as automobile insurance or life insurance, cybersecurity insurance has limited historical data. For instance, the concept of life insurance was first proposed by the Amicable Society for a Perpetual Assurance Office in 1762, marking the beginning of life insurance development. On the other hand, the earliest form of cybersecurity insurance dates back to 1977 when AIG introduced a product known as third-party liability insurance, which had many shortcomings in coverage and insurance responsibilities. This shorter history of cybersecurity insurance development results in insufficient experience, making it one of the key reasons for the lack of well-defined standards in the industry. High Confidentiality: Issues related to cybersecurity often involve sensitive data belonging to individuals or enterprises. Typically, this data directly affects individuals' futures and enterprises' development, making it impossible to disclose to the public. Without data support, the application value of cybersecurity insurance is significantly reduced, leading to a lack of representative and referenceable case studies.

2.2 Difficulty in Defining Data Assets

The current difficulty in defining data assets can be summarized as follows:(1). Ownership Rights of Data Assets: In the digital economy era, the concept of "data as assets" has been widely accepted and recognized by society. However, since data is considered an asset, it is necessary to determine its ownership to facilitate subsequent management. However, determining the ownership of data assets is currently the biggest challenge in data asset management. Firstly, data is stored electronically, which makes it susceptible to loss, deletion, dissemination, and replication, posing significant difficulties in determining ownership rights. Secondly, unlike physical assets that are consumed during circulation, data assets do not diminish; instead, they accumulate, which further complicates the definition of data assets. Lastly, there is a distinction between producing data and owning data. For example, the data generated by users when shopping online or chatting on software platforms is not owned by the users but is considered a core asset by internet companies. If internet companies exploit users' produced data for profit without their prior knowledge, because users do not have ownership rights over such data, it is challenging for the insurance industry to determine compensation liability.(2). Data Security and Personal Privacy Protection Issues: Personal privacy protection poses another major challenge in data management. Typically, when users log into a software application, the platform will display a "user agreement" promising not to misuse data. However, in reality, these agreements often lack effective enforcement, and few companies genuinely adhere to them.(3). Difficulty in Data Asset Evaluation: Data assets may depreciate over time without limitation, and they can be used indefinitely. However, the benefits derived from their use do not necessarily decrease over time, making it challenging to assess the value of digital assets. These three points are the main reasons for the difficulty in defining digital assets.

2.3 Difficulty in Safeguarding Cybersecurity Data

The main reasons for the difficulty in safeguarding cybersecurity data are as follows:(1). Inability of Cybersecurity Technology to Keep Pace with Advancements in Hacker Attack Techniques: Hackers constantly search for vulnerabilities in cybersecurity technologies to infiltrate networks. Consequently, their techniques evolve rapidly, while cybersecurity technology development progresses at a much slower pace. As a result, ensuring absolute security for networks becomes challenging.(2). Vulnerability to Human Factors: Many instances of network data breaches occur due to human error, such as setting system passwords too simplistically, insufficient employee awareness of network security, and failure to encrypt sensitive files. These issues increase the difficulty in safeguarding cybersecurity data.(3). Complexity of the Cybersecurity Environment: With the advent of the big data era, China's information technology has advanced rapidly, with emerging technologies such as the Internet of Things, blockchain, cloud computing, and big data providing significant convenience for enterprise modernization. However, these technologies also contribute to a more complex network environment, significantly increasing the difficulty in safeguarding cybersecurity data. Regulatory authorities and enterprises often need to invest more costs and resources to address potential threats hidden in obscure corners.

3. Strategies for the Development of Cybersecurity Insurance in the Digital Economy Era

3.1 Strengthen Government Regulatory Oversight

Government oversight is indispensable for cybersecurity insurance in the digital economy era. Firstly, government departments should establish a sound policy and standards system for cybersecurity insurance. This includes enhancing cybersecurity insurance policy systems, strengthening the construction of cybersecurity infrastructure, promoting innovation and development in cybersecurity insurance, guiding enterprises to develop insurance products that cater to cybersecurity characteristics, and providing support such as insurance tax incentives and purchase subsidies to incentivize individuals and enterprises to purchase insurance. Secondly, it is essential to establish and improve cybersecurity insurance standards and regulations to support collaboration between cybersecurity companies and insurance companies. This facilitates the establishment of standardized insurance processes and after-sales services tailored to the actual cybersecurity environment, enhancing the practicality and rationality of insurance, and ensuring that cybersecurity insurance can effectively be implemented and utilized in the digital economy era.

3.2 Strengthen Management of Insurance Companies

In the digital economy era, there are several management measures for cybersecurity insurance companies:(1). Strengthening the Management of Insurance Personnel: Enterprises should conduct regular training activities to enhance the professional competence of insurance personnel. In addition to ensuring that employees have a thorough understanding of insurance regulations and responsibilities, they should also be educated on different types of cybersecurity risks. This enables insurance personnel to quickly identify network risks and formulate targeted insurance plans. Training should incorporate practical cybersecurity cases to help employees develop correct cybersecurity awareness and enhance their experience in managing network risks.(2). Strengthening Follow-up Visits to Insured Enterprises: Ensuring service quality is crucial for the development of enterprises. Since cybersecurity insurance is fundamentally a service industry similar to life insurance, a positive service attitude is essential. After establishing cooperation, enterprises should strengthen supervision of partners and provide regular technical guidance, maintenance, and repair services. This not only increases partner satisfaction but also reduces the probability of insurance claims, thereby playing a crucial role in improving enterprise economic efficiency.

3.3 Increase Management of Network Security Protocols

Measures to increase the management of network security protocols include:(1). Transport Layer Security Protocol: This protocol encrypts transmitted data to ensure confidentiality and integrity during transmission, preventing data theft or tampering. It can also use digital certificates to verify the identities of communicating parties, preventing man-in-the-middle attacks. The protocol undergoes continuous version upgrades and security vulnerability fixes to ensure its security.(2). IP Security Protocol: This protocol enables transparent encryption without modifying upper-layer applications. It supports flexible access control policies, allowing access control based on source and destination IP addresses.(3). Virtual Private Network (VPN) Technology: This technology establishes encrypted tunnels to ensure secure data transmission over public networks. Typically, it combines authentication and access control mechanisms to ensure that only authorized users can access internal network resources.

Conclusion

In the digital economy era, the development of cybersecurity insurance presents both opportunities and challenges. How to navigate through these challenges with the right strategies and seize the opportunities for development is a key issue that cybersecurity insurance companies need to focus on. In today's era, the digital economy has become a key force in reshaping global element resources, restructuring global competitive advantages, and reshaping the global economic structure. The vigorous development of the digital economy in China contributes to enhancing the operational efficiency of enterprises, opening up multiple business paths, and improving both economic and social benefits. This enables enterprises to stand firm in the fierce market competition.

References

[1] Zhou, D., Tian, X., & Wu, Y. (2023). Implementation and evaluation of financial network security level protection schemes under the development of the digital economy. *Tsinghua Financial Review*, 2023(5), 107-112.

[2] Qin, X. (2024). Strengthening industrial network security bottom line to ensure sustainable development of the digital economy. *Digital Economy*, 2024(3), 70-73.

[3] Tang, J., & Liu, R. (2023). Research on the optimization of underwriting scope of cybersecurity insurance in China in the era of the digital economy. *Journal of Insurance Vocational College*, 2023, 37(3), 5-13.

[4] Jia, X. (2023). Research on network security guarantee for digital economy development in Heze City based on big data. *Journal of Shandong Agricultural Engineering College*, 2023, 40(9), 34-40.

[5] Guo, X. (2023). Strengthening technological innovation in network security to build a solid foundation for the security of the digital economy. *China Information Security*, 2023(4), 55-56.