Ludmila Gumenyuk
Department of Insurance, Banking and Risk Management,
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
E-mail: mila_gumenyuk@knu.ua
ORCID: https://orcid.org/0000-0002-2803-913X

Cyber insurance: modern requirements

Abstract

The purpose of this article is to outline current trends in the development of cyber insurance in the world and in Ukraine. Modern information wars and a significant increase in cyber-attacks over the past three years (2019–2021) indicate a low level of protection of critical infrastructure, data storage and personal information, so the development of cyber insurance as an effective protection tool is a priority today. *Methodology*. The article used methods of data analysis and synthesis to prepare the information base for defining the concept of cyber insurance; comparison of domestic and foreign publications to describe key features of cyber insurance; scientific induction and deduction to create recommendations for the spread of cyber insurance. *Results*. The results of the study indicate a high degree of danger of cyber risks in the modern world, as their variety is growing exponentially. That is why an effective mechanism for protecting the data of states, authorities, businesses and individuals must include cyber insurance. In addition, insurance companies need to develop policies with an individualized approach to each client, because the characteristics of digital behavior and the security state of the IT structure may differ. *Practical implications*. The article substantiates the provision of services to create an effective set of services against cyber risks and proposes a mechanism of interaction between insurance market participants on the vector of cyber insurance. The article classifies the main types of cyber risks for the business segment and individual clients, highlighting the most critical and dangerous ones. *Value/originality*. The results of the study allow insurance companies to create relevant products, prepare customers for modern challenges and prevent cyber-attacks, and government agencies to regulate relations in the field of cyber insurance.

Keywords

Cyber insurance, cyber risk, risk management, digitalization, cyber-attack, cyber protection, cyber protection

JEL: G22

DOI: https://doi.org/10.30525/2500-946X/2021-4-5

1 Introduction

In today's environment of uncertainty, it is important for any business to adapt to the challenges of the external environment. Thus, during the Covid-19 pandemic, all participants in economic relations felt not only the direct consequences of the crisis (medical burden), but also the indirect ones (economic losses), but a special place during this period was occupied by cyber risks. It was in the last two years that the existing problems in the field of IT infrastructure and data protection became clearer. The article examines the chronology of the formation of cyber insurance and identifies the features of each stage. This approach will allow us to anticipate and prepare for the global challenges of cyber insurance.

Cyber insurance is a small but growing market sector. As cyber-attacks become more frequent and dangerous, people and organizations are looking for cyber insurance to protect them from these risks. However, the cyber insurance industry faces significant challenges, including a lack of historical data, an inability to predict the future of cyber risk, the possibility of large cascading losses, uncertainty among market participants as to what exactly such policies cover, and legal inconsistencies. Therefore, the future growth of the market depends on how these problems are resolved.

In the process of providing insurance services, the client should be the central subject of the relationship. This approach allows not only to retain existing clients, but also to expand their number and increase their loyalty. This scheme is also relevant for cyber insurance, because today data privacy is one of the most promising vectors of science. In order to effectively establish relations between all participants in the relationship arising in the process of cyber insurance, it is necessary to describe its principles, such as: comprehensiveness, rapid response, prevention, measurability in time, compliance with international standards, compliance with the damage, comprehensiveness.

The specificity of cyber insurance is manifested in the expediency of cooperation between insurers and consultants at all stages of the insurance contract, from the conclusion to the onset of the insured event and payments on it. The article offers a SWOT-analysis of cyber insurance, which determines the optimal format of relations between all subjects of cyber insurance.

2 The evolution of cyber insurance

The importance of digital transformation in all sectors of the economy was repeatedly confirmed during 2020. Most processes within companies have changed under the influence of COVID-19, which has forced businesses to move to a remote format. Along with this transition, companies have faced the challenge associated with these changes: protecting against cyber-attacks, as well as preserving the integrity of customer data used by the company. Today, one of the world's tools for protecting and preventing digital incidents is cyber insurance. Since the middle of the 20th century, the amount of data has grown exponentially, causing an information boom. Businesses depended directly on their hardware and software, but sometimes cyber incidents occurred even with a large number of security mechanisms in place.

The first step in the evolution of cyber insurance was to change the business itself. The main challenge facing businesses was the re-engineering of business processes in accordance with the need to expand production and improve the quality of the final product. Thus, the traditional business model has been replaced by the digital model, which means using digital technology to identify new sources of income and monetize these processes. The introduction of innovative systems led to an increase in the amount of data generated and received by organizations, so storing physical information became impractical and was replaced by digitization, the digital transfer of data encoded in discrete signal pulses.

Another element in the evolution of cyber insurance has been a set of measures to improve information systems to ensure rapid access to them. At this stage, the use of the Internet as a data transmission channel became widespread. With the development of the integration capabilities of this channel, cloud services and mobile access to information were introduced. Cloud services made it possible to move computing operations to Internet servers, while reducing the load on their own systems. The need for fast access to information led to the creation of mobile versions of software and data storage.

At the current stage of cyber insurance development, the trend of providing customers with exclusive products has transformed into giving consumers special access to various platforms. The need for organizations to respond quickly to market innovations has led to the emergence of shadow software within companies, which is often created and launched in violation of established norms and without appropriate legal support (O'Donnell, 2017). The ability to use PCs to manage information systems allows access to data from any device at any time. This upgrade was also the basis for the "Bring your own device" (BYOD) concept – recommending that employees use their own devices to reduce workplace costs. The Internet of Things has become an organic source of synchronization between software, the Internet, and technological devices – a system of networked objects that exchange data about their state with the external environment using embedded technologies. In addition, the transition to innovative business options has provoked changes in the interaction of not only the business client, but also the business employee.

3 Principles of cyber insurance

In order to summarize the approaches to the basics of cyber insurance, it is necessary to consider the principles of cyber insurance, which provide the most accurate definition of its main characteristics. Also, the issue of coverage of policyholders' losses from the occurrence of cyber-incident insurance attacks has not been sufficiently studied. The lack of global experience makes it difficult to implement and disseminate cyber insurance, as policyholders often do not understand what risks and losses an insurer can cover in the event of a cyber-attack. Insurers often need more time and money to accurately identify risks than the period over which the attack itself occurs and the amount attackers charge to maintain data integrity. With this in mind, insurers face the challenge of integrating with cybersecurity organizations to develop a variety of insurance products for different stakeholders. For example, the first cyber insurance contracts were signed by private companies in the U.S. in 2010 as a way to reduce the liability of owners to retain information about their customers (Biener & Eling & Wirfs, 2015). Since 2013, there has been active growth in this type of insurance due to the massive outage of U.S. corporate and government resources, so cyber insurance contracts have also undergone significant changes, adding to the traditional point of information retention an expanded range of possible attacks, reputation and in-house investigation.

To ensure an effective cyber insurance mechanism, it is necessary to act in accordance with principles that bring the client's cyber security conditions as close as possible to the optimal ones. The basic principle of cyber insurance is comprehensiveness, an overall assessment of the insured's condition with a detailed review of the functioning of its business model to understand the full list of possible sources of threats. According to the identified risks, the insurer offers a unique policy, with a set of relevant types of risks

and possible losses on them, with a set of products suitable for a particular insured. The next principle is quick response, which means close cooperation of the parties involved in order to immediately identify the fact of the insured event and transfer it for qualification to a consulting organization to minimize losses. Prevention is another principle on which cyber insurance is based and means learning from historical flaws in systems and creating conditions to prevent the occurrence of an insured event or taking precautions to reduce the likelihood of a cyber-attack and damage. Measurability over time is also an important principle, because the insurer and the insured must determine the dimensionality of the period of time for which the insurance contract will be concluded, because this type of insurance uses additional software to monitor and analyze the current state of the object, conversion or renovation. The next principle is compliance with international standards of data storage and processing, due to the lack of legislation on cyber insurance in many countries, which means that when an insured event occurs, they will be the regulatory basis for making decisions on the allocation of losses/costs. It is worth noting that all the principles of cyber insurance are interrelated and complex. The last principle is damage correspondence, which means the ratio of the amounts of compensation received separately and the damage broken down by the categories to which they belong. That is why the final amount of compensation is detailed according to the areas of future funding for projects affected by cyber-attacks.

In conclusion, it should be noted that cyber insurance has transformed into a separate type of insurance as a result of the rapid development of information systems, the growth in the volume of information generated and stored by individuals and legal entities, as well as the increasing importance of privacy of personal data, which aims to protect policyholders in the event of cyber incidents.

4 Future of cyber insurance

In today's environment, the protection of information systems, personal data and networks is one of the most important tasks of international importance. One of the options for creating a comprehensive protection system is the cooperation of government agencies, international organizations, IT organizations and insurance companies, because such a solution will not only reduce the probability of an attack, but also minimize losses in the event of an attack. But the problem in implementing such a system is the lack of appropriate institutional and legal support. This is why creating effective cooperation will reduce the threat posed by cyberattacks.

Also, the development of cyber insurance is hampered by a number of other problems that require a detailed plan of action:

1. the absence of established laws or other regulations governing the relationship between the insurer and the insured in the field of cyber insurance;
2. there is no clear classification of cyber insurance products, there are no unified norms and standards for their calculation;
3. low solvency of the insured under the operational type of business process management;
4. the lack of coordinated common interests between the state regulator and insurers, because one of the priority tasks of the state is to promote cybersecurity of the country, especially in the context of digitalization of the economy, while insurance companies are commercial organizations for profit;
5. the difficulty of proving the fact of deliberate cyber-attack;
6. insufficient level of trust of individuals and legal entities in the innovative type of insurance.

By defining the range of problems and identifying weaknesses, it is possible to develop ways to solve them, as well as to create a further plan for the development of cyber insurance and its prospects. To date, the following priorities can be identified:

1. ensuring the necessary conditions for policyholders, namely the creation of a unified regulatory framework;
2. increasing public confidence in cyber insurance and proving its effectiveness;
3. creating universal insurance policies for different groups of cyber risks, depending on the characteristics of the object of insurance;
4. the creation of a unified register of cyber attacks with an indication of their characteristics and details of the damage caused.

To improve the existing lines of business, as well as to predict possible scenarios when launching a new type of activity, an effective tool is the SWOT analysis, which includes a description of strengths and weaknesses of the project, its opportunities and threats. Since cyber insurance is an innovative activity, this analysis will show the directions of development of this type of activity and the problems that should be paid attention to for its successful development.

Based on the analyzed matrix of strengths and weaknesses of cyber insurance, we can identify the main obstacle to its active implementation – innovation and lack of consolidation at the legislative level.

5 Conclusions

This article reviews the chronology of cyber insurance development, which has been divided into 3 stages: digitalization (creation of digital devices with the establishment of their mass production), fast access (Internet and cloud services) and exclusivity (IoT, cyber-attacks and other risks). Throughout these phases, from the 1970s to the present, there has been a significant growth in the number and types of digital devices, an increase in the capabilities of

TABLE 1 SWOT analysis of cyber insurance

Strengths	Growing demand for cybersecurity services; High level of automation of insurers' service systems; high level of confidentiality of customer data; lower operating costs; ability to manage risk in real time; contributing to a reduction in cyberattacks.	Weaknesses	Lack of a clear classification of cyber insurance products; insufficient level of development of regulatory and legal support; low level of public confidence in insurance; availability of uncontrolled operating systems, on which insurers have no direct influence, appropriate technological equipment; exclusion of potentially insolvent insurance organizations from the pool of potential policyholders.
Opportunities	Protection by the state, taking into account the latest course towards digitalization; expansion of sales channels; the possibility of reducing the likelihood of human error, through the involvement of insured professional consultants; creation of new products (both universal and exclusive) to meet the needs of customers; insurance reform.	Threats	Probability of fraud and risk manipulation; the difficulty for insurers to prove the fact of a deliberate cyber incident with the corresponding consequences; violation of traditional insurance procedures with the omission of certain procedures; continuous improvement in both cybersecurity and cyberthreat tools; high level of losses; formation of new types of insurers (other industries/methods).

handheld computers, the spread of the Internet, and the digitalization of all economic processes.

The article proposes and characterizes the principles of cyber insurance, including comprehensiveness, rapid response, prevention, measurability in time, compliance with international standards, compliance with damage. Cyber insurance also covers the costs of such insured events that are related to targeted attacks, cyber investigations, the occurrence of a specific cyber incident, inconsistency in the content of information published by the insured, cyber claims, disconnection, non-targeted attack.

By defining the range of problems and identifying weaknesses based on the analysis, it is possible to develop ways to solve them, and to create a further plan for the development of cyber insurance and its prospects. To date, the following priorities can be identified: ensuring the necessary conditions for policyholders, namely the creation of a unified regulatory framework; increasing public confidence in cyber insurance and proving the effectiveness of its implementation; formation of universal insurance policies for different groups of cyber risks, depending on the characteristics of the object of insurance; creation of a unified register of cyber attacks with their characteristics and details of damage.

Thus, creating a high level of protection of information systems, networks and data transmission channels is one of the highest priorities for modern enterprises. In this context, cybersecurity is a set of practices and measures to protect systems, programs, networks, data transmission channels and data stores from cyberattacks. To implement all these procedures, companies create functional units or hire specialized organizations, which, in turn, process all the features of business processes and identify weaknesses in these systems, identifying them as cyber risks.

References

[1] Allianz Risk Barometer 2022 (2021). E-source: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2022.pdf
[2] Biener, C., Eling M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. E-source: https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf
[3] Collin, J., Hiekkanen, K., Korhonen, J. J., Halen, M., Itala, T., & Helenius, M. (2015). The Impact of Digitalization on Finnish Organizations. E-source: https://aaltodoc.aalto.fi/bitstream/handle/123456789/16540/isbn9789526062433.pdf?sequence=1&isAllowed=y
[4] Cyber claims study, NetDiligence (2014). E-source: https://netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf.
[5] O'Donnell, J. (2017). IDC says get on board with the DX economy or be left behind. E-source: techtarget.com