Role of Cyber Insurance in Managing Digital Risk

Abdurasulova Xadichaxon Ravshanbek qizi
Tashkent State University of Law
xadichaabdurasulova06@gmail.com

Abstract

In an increasingly digital world, government, businesses and individuals found themselves facing a new wave of challenges — the ones spurred by the digital age. Data breaches, ransomware attacks, and other cyber incidents can have devastating consequences, ranging from financial losses to reputational damage. In this context, cyber insurance has emerged as a critical component of a comprehensive risk management strategy. In this article, we will explore the significance and implications of cyber security insurance in today's digital landscape. By analyzing the importance of cyber insurance in an increasingly digital world, we get some information about its role and necessity; we also acquire the knowledge about strong and weak sides of cyber insurance.

Keywords: Cyber security, Cyber threats, Digital Risk, Cyber Insurance, Managing Risks, Digital attacks, Cyber Law

I. Introduction.

Governments and businesses are struggling to cope with the scale and complexity of managing cyber risk. Over the last year, remote working, rapid digitalization and the need for increased connectivity have emphasized the cyber security challenge. As the pursuit of approaches to prevent, mitigate and recover from malicious cyber activity has progressed, one tool that has gained traction is cyber insurance. If it can follow the path of other insurance classes, it could play a significant role in managing digital risk [1]. Therefore, this article aims to explore the role of cyber insurance in the digital landscape and its importance in preventing cyber-attacks.

The role of information technology in the daily life of a person and the activities of operations, allowing you to save not only financial resources, but also

time. At the same time, the development of information technologies and their more active introduction into private and business practices has the opposite side: the task of preventing cyber-crimes are being updated. Not only the number of cyber-attacks are rising, but also the level of their complexity, the scale of the losses associated with them. At the same time, the demand for cyber insurance is also increasing as a tool for compensating financial losses of subjects of information systems, resources and technologies, as a method of information risk management [2]. Due to the growing number of cybercrimes around the world and the fact that cybercrime prevention is one of the most fundamental problems for all countries, through this article there is a need to consider the basics of the legal development of the Cyber Insurance in Uzbekistan.

By examining the experience in cyber insurance in foreign countries, this article analyses importance of cyber insurance in managing informational risks and its problems.

II. Methodology

To analyse the impact of cyber insurance on managing digital risks, the research methodology for this article adopted a mixed-methods approach. This approach combines both quantitative and qualitative data collection techniques to provide a comprehensive understanding of the research topic.

The study began by conducting a systematic literature review of international legal frameworks related to the Cyber insurance. The article includes also scientific articles, research papers, reports, academic journals and conference proceedings, which provides information to understand the field of Cyber Insurance in Managing Digital Risk.

In the article, the analytical method used to compare and evaluate the problems and potential solutions.

III. Results

The assessment of the international norms and current state of cyber insurance reveals both opportunities and challenges in using cyber insurance to

minimizing digital risks and cyber-attacks. The current evidence about the ability of cyber insurance to improve cyber security practices is limited. There is the potential for the cyber insurance market to learn from other insurance markets to increase uptake, although understanding the depth of these connections requires further enquiry.

Analyzing existing legal framework in USA and Europe, this article provide the state of the cyber insurance market and the role of insurance in advancing cyber resilience.

The analysis of international norms highlights the weak side of cyber insurance is that there is no clear existing norm to date regarding the regulation of cyber insurance and what it covers. However, while it is not sufficiently regulated in the legislation, it is widely used in American and European countries to protect against cyber threats, and we can see that it is giving its result in reducing digital risks.

As the threat of cyberattacks against applications, devices, networks, and users grows, cyber insurance has become an essential safeguard for all companies. The potential compromise, loss, or theft of data can have significant consequences for a business, ranging from erasing customer loyalty to reputational damage and financial loss.

The result of these analysis e-commerce businesses, in particular, can significantly benefit from having cyber insurance coverage, as any downtime resulting from ransomware attacks or other cyber threats can significantly negatively impact their financial standing.

Moreover, enterprises may be legally responsible for any harm resulting from losing or stealing third-party data. By obtaining a cyber insurance policy, businesses can mitigate their risk exposure to cyber events and receive support in addressing security incidents.

IV. Discussion

Cyber risk has been described as the "biggest, most systemic risk" facing the insurance market in the last half century. It essentially encompasses any risk arising out of the use of technology and data and, in this digital age, affects virtually every organisation around the world [3].

The idea either of "cyber insurance", taking the form of a standalone cover or as an enhancement to conventional lines of insurance, first emerged around 20 years ago, primarily in the US. One of the main reasons for the active development of this segment of insurance services is associated with the introduction of certain legal norms in the field of personal data protection.

The Federal Information Security Modernization Act (FISMA) is one of the cyber security laws in US passed in 2002. It requires federal agencies to implement security controls to protect their information systems and data.

They aim to ensure that federal agencies have the necessary measures to protect the confidentiality, integrity, and availability of the information they collect, store, and use.

They also require agencies to establish an information security program that includes regular risk assessments, security testing and evaluations, incident response planning, and continuous monitoring of security controls [4].

The Cybersecurity Information Sharing Act (CISA) is a law passed by the United States Congress in 2015 that encourages private companies to share information about cyber threats with the government and provides liability protections for companies that do so.

CISA aims to improve the sharing of information about cyber threats between the government and private sector to protect critical infrastructure and national security from cyber-attacks. It allows private companies to share cyber threat information with the Department of Homeland Security (DHS) and other federal agencies and enables the government to share cyber threat information with private companies.

A key aspect of the evolving cyber risk landscape is the on-going development of data privacy law in Europe, which is seeing organisations face greater liability risks in relation to the use of data than was previously the case.

Stricter rules will be imposed on data controllers in relation to data subject consent, data profiling, data handling and compliance. These rules will be enforced by reference to aggressive mandatory reporting requirements and potentially heavy penalties for contravention [5].

To understand why cyber insurance is important, let us first ask: what is cyber insurance? Cyber insurance allows companies to transfer some of the financial risk associated with cyber incidents to an insurer [6].

Cyber insurers can help to identify particular experts to mitigate risk [7]. Insurers can quickly assemble teams with relevant expertise to support their clients before, during and after an incident [8]. This includes forensics teams and breach counsel, and public relations and other cyber crisis responders. Companies can often gain access – for example, free access or direction to key services – to these resources through their cyber insurance policy [9].

Cyber insurance is a valuable asset for any business dealing with online electronic data. In today's digital age, sensitive customer information such as contact details, sales records, personal data, and credit card numbers are all attractive targets for cybercriminals. This is where cyber insurance comes in to provide protection. One of the biggest reasons why cyber insurance is necessary is the potential financial loss that can occur in the aftermath of a cyber incident. Cyberattacks can result in significant financial costs, including expenses related to investigating the breach, notifying affected individuals, and providing credit monitoring services. Additionally, there are legal fees and potential fines that may arise from compliance violations or failure to protect customer data. Without proper insurance coverage, businesses may find it challenging to recover from these financial burdens.

The scope of cyber insurance is an essential aspect to consider when assessing coverage and risk mitigation strategies in today's digital landscape. With the increasing frequency and sophistication of cyber threats, it has become crucial for businesses and individuals to protect themselves against potential financial losses resulting from data breaches, cyber-attacks, or other related incidents. Cyber insurance policies aim to provide coverage for a wide range of cyber risks, including but not limited to data breaches, business interruption, network security liability, and regulatory fines.

To understand the scope of cyber insurance, it is important to consider the various coverage options available. At present, forms of cyber insurance are many and varied, but typically include cover for loss arising from:

1. Damage to Digital Assets (data and programmes);
2. Non-physical business interruption and extra expense;
3. Cyber extortion;
4. Privacy Liability;
5. Confidentiality Liability;
6. IT Liability;
7. Regulatory fines, costs and expenses;
8. Crisis Management (mitigation) costs, including notification expenses, forensic expenses, public relations costs, credit monitoring and other assistance costs [10].

Although cyber insurance has many strengths and benefits, nowadays it has its own weak sides, such as the cyber insurance market is like other markets that are not yet fully developed in that (1) demand is inconsistently informed; (2) uncertainty and behavioural distortions impede decision-making; (3) common vocabularies are not broadly adopted; (4) suppliers' solutions are not standardised; (5) historical knowledge is limited; (6) industry regulators (such as

the FCC in the U.S.) are unsure of their role and what to do; and (7) the ecosystem is fragmented.

As a result, participants cannot appreciate the nature of the risk and the efficacy of preventive measures. Informational asymmetries create issues related to moral hazard and adverse selection [11].

While cyber insurance is frequently mentioned as an appropriate risk transfer mechanism, it is only recently that cyber insurance has become a marketable offering. Therefore, the concept of cyber insurance has not yet been introduced in the legislation of Uzbekistan. Although the regulation of cyber insurance was established in the decision of the president of the Republic of Uzbekistan in 2019 "On measures to reform the insurance market of the Republic of Uzbekistan and ensure its rapid development", our legislation has not yet regulated this concept.

In terms of managing digital risks, Uzbekistan has implemented legislation to cyber security. The law focuses only general rules and obligations of competent authorities in managing digital risks in cyber world. This law does not provide information about the concept of cyber insurance. As the demand for cyber insurance is rising, and it is the only measure to minimize the digital risk, there is need to improve legal landscape of cyber security internationally.

In order to introduce cyber insurance into the legislation of Uzbekistan, we consider that the following issues must be resolved:

1. The concept of cyber insurance should be described;

2. It is necessary to specify what damages cyber insurance covers;

3. The role of cyber insurance and the limit of the money paid by the insurance should be established in the case of criminal damages;

4. Cyber crimes and their types should be revised in our legislation;

5. If the data is obtained by cyber attacks to the database of enterprises, the issues of responsibility for the enterprise must be resolved;

6. What the role of cyber insurance should be considered when the electronic bases of individuals and legal entities are attacked;

7. It is necessary to form a list of types of cyber attacks that cyber insurance does not compensate. (e.g. as a result of military attacks).

As it is a relatively new offering for insurance companies, insurers in recent years have spent a great deal of time clarifying what cyber insurance is, what it does and does not cover, and how to best build profitable portfolios. Some of those issues are covered in this section. In addition, there are further questions about the purpose of cyber insurance, how it functions in practice and the unique challenges it faces to become a fully mature insurance sector with high uptake [12].

Conclusion

This article has explored the legal framework cyber insurance in managing digital risks. The research revealed both strong and weak areas in cyber insurance market. By analyzing international norms, we have witnessed that a special norm that regulates cyber insurance has not yet been developed.

Few insurance companies are ready today to offer a high-quality, system-dark product aimed at protecting customers from cybercrime and managing digital risks. The toolkit has not been worked out yet, the almost complete absence of payment practice makes it impossible to check all insurance cases and types of coverage for system errors. To date, there is no legislative framework and judicial practice for the widespread introduction of this type of insurance. So far, there are not enough specialists in Uzbekistan and insurance companies, who have an idea of the structure of risks.

References

1. Jamie MacColl, Jason R C Nurse and James Sullivan. (2021). Cyber Insurance and the Cyber Security Challenge. RUSI Occasional Paper. ISSN 2397-0286 (Online). Available at: https://static.rusi.org/247-op-cyber-insurance.pdf
2. Cyber Risks and Insurance. (2016). International Underwriting Association of London Limited. Available at: https://www.maritimelondon.com/wp-content/uploads/2016/01/005_Cyber_Risks_Combined_110116.pdf
3. Federal Information Security Modernization Act of 2014 U.S.C. https://www.congress.gov/bill/113th-congress/senate-bill/2521
4. Marco Davi. (2010). Cyber security: European strategies and prospects for global cooperation.
5. James Sullivan and Jason R C Nurse. (2020). Cyber Security Incentives and the Role of Cyber Insurance. *Royal United Services Institute for Defense and Security Studies.* RUSI is a registered charity (No. 210639). Available at: https://cesmar.it/wp-content/uploads/2023/04/2020-cyber_insurance.pdf7.
6. Cyber Risks and Insurance. (2016). International Underwriting Association of London Limited. Available at: https://www.maritimelondon.com/wp-content/uploads/2016/01/005_Cyber_Risks_Combined_110116.pdf
7. Daniel W Woods and Tyler Moore. (2019). Does Insurance Have a Future in Governing Cybersecurity? *Global Cyber Risk Perception Survey*. Available at: https://ieeexplore.ieee.org/abstract/document/8833500
8. HM Government, 'UK Cyber Security', p. 17. Available at: https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2023/uk-cyber-security-sectoral-analysis-2023
9. James Sullivan and Jason R C Nurse. (2020). Cyber Security Incentives and the Role of Cyber Insurance. *Royal United Services Institute for Defense and Security Studies.* RUSI is a registered charity (No. 210639). Available at: https://cesmar.it/wp-content/uploads/2023/04/2020-cyber_insurance.pdf
10. Sauhin A Talesh. 'Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Business', Law and Social Inquiry (Vol. 43, No. 2, Spring 2018), p. 417. Available at: https://www.law.uci.edu/faculty/full-time/talesh/Talesh-2018 Law_Social_Inquiry%20Cyber.pdf
11. Cyber Insurance as a Risk Mitigation Strategy Copyright. (2018) *The Geneva Association, MIT, and The Boston Consulting Group*. Available at: *https://media publications.bcg.com/pdf/cyber_insurance_as_a_risk_mitigation_strategy.pdf*
12. James Sullivan and Jason R C Nurse. (2020). Cyber Security Incentives and the Role of Cyber Insurance. *Royal United Services Institute for Defense and Security Studies.* RUSI is a registered charity (No. 210639). Available at: https://cesmar.it/wp-content/uploads/2023/04/2020-cyber_insurance.pdf