Financial and Economic Sustainability
FINECS ISSN-2181-1636 Vol. 6, Issue 1, Feb, 2026
https://finecs.kit.uz



CYBER-RISK INSURANCE ISSUES IN THE CONTEXT OF DIGITALIZATION OF THE ECONOMY

Norov Zarif Shamsiddinovich,
General Director of JSC "Kafolat insurance company", Tashkent
https://doi.org/10.5281/zenodo.23883981

Abstract. As a result of the acceleration of the digitization process, cyber risks, cyber threats, and cyber crimes have become a dangerous enemy of humanity. It is important to identify cyber risks, assess risks by classifying them into categories, fight against cyber crimes, and protect yourself through insurance packages. Moreover, creating a protective wall against cyber crime by taking measures to ensure security in the enterprise, ensuring data security in the internal system, and taking measures to ensure information security at the state level is an urgent issue today. This article describes the analysis of the results obtained as a result of the identification of cyber risks, ensuring cyber security in the government and industrial sectors, and the active use of cyber insurance. In addition, the article describes the scope of cyber insurance coverage divided into categories of first-party losses, incident response costs, and third-party losses.
Key words: digitization, cyber risk, cyber threat, cyber crime, cyber risk, cyber insurance, cyber security

Introduction.

In financial markets, the widespread use of new digital tools and technologies shapes the boundaries and characteristics of the financial-economic environment, raising new challenges with emerging risks for its participants. Digital financial technologies form the basis of digital platforms that drive the transformation in service delivery. The proliferation of online payments, lending, and money transfers in developing economies is considered a growth trend in the financial technology market. Simultaneously, the increasing frequency and severity of cyberattacks underscore the importance of ensuring cybersecurity and mitigating the associated costs. For instance, the daily accumulation of losses resulting from the theft of trade secrets or personal information, data breaches, intellectual property theft, and the depreciation of corporate brands continues to rise. Addressing the tasks of digitizing the economy involves assessing the risks of operational entities and taking proactive measures to counter cyber threats, making cybersecurity insurance from cyber risks an increasingly pressing issue.

The rapid development of digital economic processes is accompanied by the emergence of cyber threats, which expand the field of tasks for ensuring cybersecurity, along with promoting digital transformation for economic growth. All economic actors utilize digital analogs at every stage, from automating workplaces to delivering products and services to customers. The involvement of digital and financial technologies poses a range of risks for entrepreneurs and citizens alike. These risks, such as "production disruption," "information security," "Cyber Risk," and "Cyber Insurance," are increasingly shaping the role of new concepts in the economy.

It is possible to understand the seriousness of the situation by reaching positive results in the economy through digitization today, together with negative statistical data. According to the results for the end of 2021, the global damage from cyberattacks amounted to $6 trillion, making it equivalent to the GDP of the third largest country after

the United States and China. The average annual growth rate of cybercrime worldwide is 15%[1]. Global spending on IT security is estimated at $150 billion in 2021[2].

The annual survey conducted by Allianz Global Corporate & Specialty (AGCS) gathers the opinions of 2,650 experts from 89 countries and regions, including CEOs, risk managers, brokers, and insurance experts. This survey, for the year 2021, marks the second time in the history of Allianz Risk Barometer surveys that cyber incidents rank first in the rating (collecting 44% of the votes), surpassing supply chain disruptions, which moved from the fourth place to the second (42%) due to cyberattacks on businesses. Natural disasters claimed the third spot (25%). Climate change witnessed the highest increase in rankings in history, moving from ninth to sixth place (17%), while the pandemic dropped to fourth place (22%) according to the results[3].

According to data provided by IBM, by the end of 2021, the average total cost of a data breach in a company will be 4.24 million dollars. The average cost per record of lost or stolen personal information was $161[4].

For this reason, many experts have argued that cyber insurance can be an effective tool to manage cyber risks that are likely to occur.

Litearture review.

Sebula, J. J. and Young, L. R. (2010) defined the aggregate of risks related to the impact of various sources that could potentially affect the technological assets, databases, or other online storage locations of a legal or physical entity as cyber risks. In general, financial institutions and insurance markets classify cyber-related risks as part of operational risk due to their association with technology and information assets. Therefore, cyber risk can be defined as part of operational risk associated with the availability, integrity, and confidentiality of technological assets and information. According to research conducted by Biener, Ch., and others (2014), cyber risk is defined as operational risk associated with the material and non-material damage to organizational assets, potential disruptions to business chains, or disruption to activities in cyberspace that threaten information assets, ICT resources, and technological assets. Consequently, cyber risks can be divided into two main groups based on the source of the threat: insider (financial loss, fraud, data breaches, and disclosure of personal information of employees) or outsider (confidential information of the company, financial operations). Through these cyber risks, companies may not only lose confidential information and funds but also compromise their reputation, contracts, and customer trust. The assessment of cyber risks also encompasses threats posed by physical individuals to ICT resources within the organization. In this regard, Boehme et al. (2018) identified and classified the following three groups that contribute to the occurrence and impact of cyber risk indicators:

a. Cyber cause → damage to digital assets.
b. Cyber cause → damage to physical assets.
c. Physical cause → damage to digital assets.

According to Ridd, J. (2002), in order to prepare a cyber insurance package, the company's general internal information database can be divided into three categories, namely IT-related information, human resources department, and financial, internal audit, legal issues.

---

[1] https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf
[2] https://www.gartner.com/en/information-technology/insights/top-technology-trends
[3] https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html
[4] https://www.ibm.com/downloads/cas/ADLMYLAZ

Varian, H. (2000) states that when creating a cyber insurance policy, the most important source of business information that the insurance company needs to know is considered, and the terms of the contract should be mutually beneficial. Therefore, analyzing the risks that may arise, increasing the level of the company's cyber resilience, and preparing solutions for insurance requires a deep understanding of the business profile, i.e., the company's main activities, customer base, geographic information, financial details, and information security budget.

According to Bodin, L. et al. (2018) analysis, information is one of the most important assets of an information company, and in the event of its theft or loss, it can lead the company to a crisis situation. In addition, information and communication technologies are becoming an increasingly important part of daily activities in the rapid development phase of digital technologies. Cyber attacks on ICT systems can result in significant financial losses.

According to Barreto et al. (2017), all cyberattacks lead to financial losses, as well as a loss of confidence in the organization's activity sector. The obligation to protect the information of third parties is specified in the laws and they are responsible for serious social, economic, and legal consequences in case of theft or disclosure of their information.

Research Methodology. In this article, cyber risks are classified in the context of digitizing the economy, providing statistics on ensuring cybersecurity in government and industry sectors, security issues, human factors in the occurrence of cyber risks, technological and systemic vulnerabilities, successful internal management, and external factors analysis. Analytical methods such as analysis, synthesis, abstract-logical and critical thinking, scientific validation, comparison, and generalization were used.

Analysis and Findings:

Given the rapid advancement of digital technologies and the increasing complexity of companies' IT infrastructures, it is imperative to recognize the significant growth in the number of cyber incidents. Data breaches, disruptions in business chains, hacking attacks, or the leakage of confidential information pose serious challenges, and the protection against cyber threats becomes crucial as a rational approach to reducing harm through cyber security measures.

The methodology for securing against cyber threats is considered a complex and challenging process, as it involves both internal and external assessments of risks. An essential aspect is the engagement of an information security (Information Security) audit company, which evaluates risks beyond the scope of insurance companies and provides conclusions tailored to the insurance company. However, the absence of comprehensive proposals for assessing complex cyber risks in the insurance market today indicates the relevance of this issue.

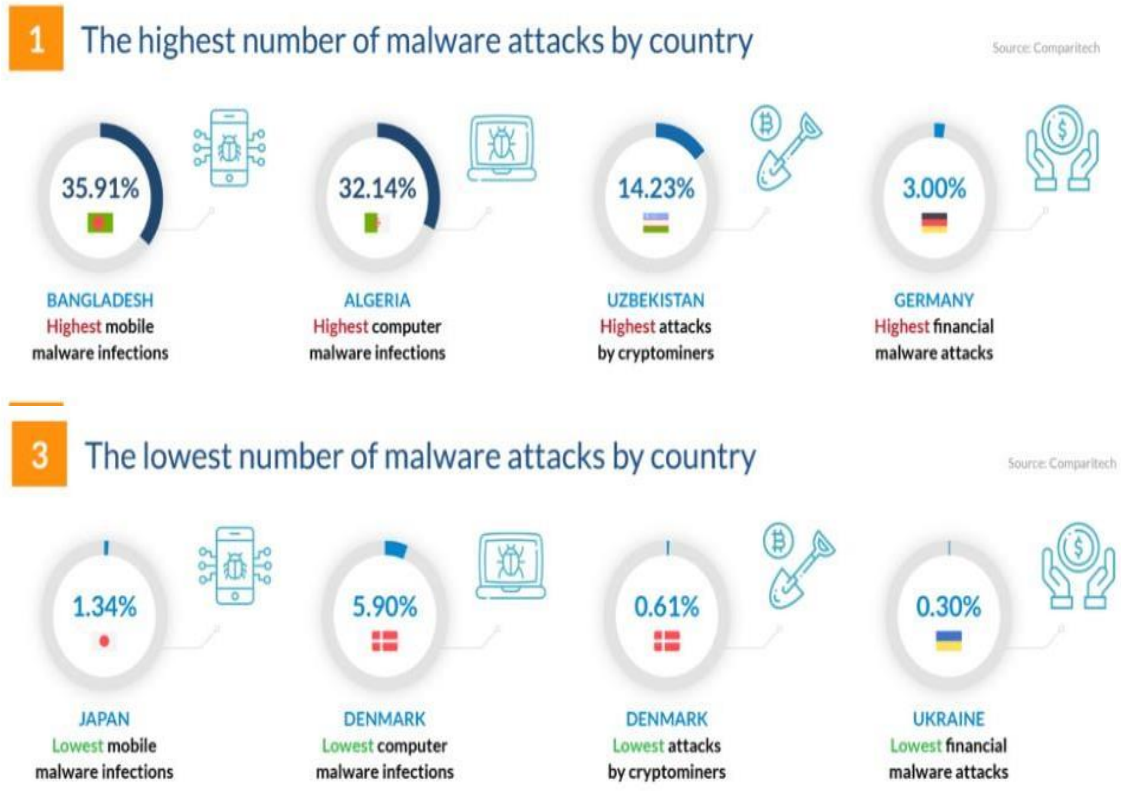
In early 2019, insurers began to offer more extensive services, additional coverage options, and potential for expansion to provide insurers with broader services. As a result, there was a significant increase in the offering of new insurance services in the insurance market. By 2022, insurance companies aiming to purchase cyber protection were striving to provide continuous security for optimal offers and quality services. Overall, the cyber insurance market continues to evolve steadily.

Developing cyber insurance classes, creating insurance policies, is one of the most challenging tasks for insurers because there are still many terms and descriptions that need to be clearly defined and classified. For example, all cyber incidents not covered in the insurance policy terms - liability and property policies would be most vulnerable.

Insurers need to clarify the need for cyber insurance coverage in terms of property or liability, that is, property or liability insurance, to provide the policyholder with adequate coverage.

Cyber insurance has already achieved significant success in the global insurance market, and its further expansion is forecasted in the future. According to the latest data, the volume of the global cyber insurance industry reached $7.8 billion in 2020. Forecasts indicate that the cyber insurance industry is expected to grow to $20 billion by 2025. Business representatives acknowledge the prominent role of cyber insurance in the market. For instance, in 2018, 75% of cyber insurance payouts in the United States were claimed by business representatives, while the remaining 25%, amounting to $500 million, were related to individuals[5].

One of the main drivers of the growth in the cyber insurance market is the increasing volume and impact of cyber incidents. According to compiled statistical data, in 2020, nearly one out of every six companies fell victim to Ransomware cyberattacks, with approximately half of them paying the ransom. Ransomware is a type of malicious software used by cybercriminals. The number of reported cyber incidents in 2020 increased by 69% compared to 2019. On average, around 2,000 cyber incident reports were announced daily in 2020[6]. The ranking of the countries most affected by cyber attacks varies depending on the specific type of threat. According to reports, Bangladesh tops the list for mobile application vulnerabilities and harmful viruses, while Algeria faces the most threatening computer virus attacks. Uzbekistan is particularly vulnerable to crypto-mining attacks, and Germany experiences the highest incidence of damaging financial software attacks.



[5] Statista. (2021). Cyber insurance – Statistics & Facts. https://www.statista.com/topics/2445/cyber-insurance/
[6] FBI. (2020). Internet Crime Report. ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Figure 1. Overview of the Global Cybersecurity Rankings Across Government and Industry Sectors, 2021 [7]

The compromise of personal information has a significant impact on both corporate entities and individuals' activities. In 2020 alone, the compromise of data resulted in the loss of over 37 billion personal records, with 82% of them being compromised due to cybercrimes. Data breaches not only affect companies and organizations but also jeopardize the personal privacy and security of individuals, exposing them to various risks. In 2020, the total cost of fraud losses related to personal deception reached $56 billion, averaging $1,100 per victim. Approximately 70% of those familiar with cybersecurity experienced cyberattacks, 69% had their personal information exposed, 64% encountered cyberbullying, and 69% faced cyberstalking[8].

As digitization accelerates, cyber threats, cyber risks, and cybercrimes pose serious economic, social, and financial risks to humanity. Identifying and categorizing cyber risks, assessing risks through risk categorization, smartly fighting against cybercrimes by using intelligent, secure, and high-quality encryption technologies, leveraging FinTech for effective protection, securing through insurance packages, examining security challenges in corporations, ensuring information security within internal systems, and ensuring national information security through the exploration of security challenges in various service sectors are considered valuable service types in creating a barrier against cybercrime. Cybersecurity expenditures are increasing globally. Within the leading sectors, the expenses for ensuring security are 11.9% for government or local government security, 11.8% for telecommunications, 11.0% for resource networks, and 10.4% for banking, indicating their prominence in terms of security within the respective sectors.



Figure 2. Description of the leading industries with the fastest growing security spending worldwide, 2021 [9]

Insurance companies currently offer insurance policies for the following types of risks: the risk of unauthorized disclosure and subsequent use of confidential information by organization employees; the risk of hackers obtaining information about bank clients, such as credit card and account numbers; the risk of funds being withdrawn from bank clients' accounts; the risk of company employees compromising confidential information; the risk of disrupting company operations due to malware on computer systems or organization websites; the risk of financial losses incurred by organizations as a result of improper data storage and handling, and so on.

[7] https://financesonline.com/cybersecurity-statistics/
[8] RiskBased Security. (2020). 2020 Year End Report.
[9] https://financesonline.com/cybersecurity-statistics/

The causes of data breaches are often cyberattacks, but according to Verizon's 2020 Data Breach Investigations Report, cyberattacks were not always the cause of data breaches. The main causes of data breaches in 2020 were as follows:

Hacking: Unauthorized access to business systems by hackers allowed them to gain access to and misuse information.

Errors: System vulnerabilities that are specific to errors, especially IT vulnerabilities, allowed third parties to gain access.

Social attacks: Social attacks, including phishing scams and other frauds targeting individuals, businesses, or organizations.

Malicious software: Hackers used malicious software to gain unauthorized access to company information from external sources.

Authorized users: Insiders with access rights who abused their company systems for financial or personal gain caused breaches. Physical individuals who obtained devices containing sensitive information also caused significant breaches.[10]

Solvency II ва Базел II ҳужжатларида келтирилган кўрсатмаларга кўра, киберхавфларни тўртта тоифага бўлиш мумкин: технология ва тизимдаги носозликлар, муваффақияциз ички муҳит, инсон омили ва ташқи омиллар.

Table 1.

Cyber risk categories[11]

Cyber Risk Category	Description
Malware	Malicious software designed to disrupt, damage, or gain unauthorized access to systems.
Phishing	Fraudulent attempts to obtain sensitive information by posing as a trustworthy entity.
Ransomware	Malware that encrypts files or systems and demands a ransom for decryption.
Data Breach	Unauthorized access, disclosure, or theft of sensitive information.
Insider Threat	Malicious or negligent actions by internal individuals posing a security risk.
Denial-of-Service (DoS)	Attempts to disrupt or suspend services by overwhelming systems with traffic.
Social Engineering	Manipulative techniques used to deceive individuals into divulging sensitive information.
Supply Chain Risk	Vulnerabilities in third-party vendors or suppliers that pose a risk to the organization.
IoT Vulnerabilities	Security weaknesses in Internet of Things (IoT) devices that can be exploited by attackers.
Regulatory Compliance	Failure to comply with laws and regulations governing data protection and privacy.

In developed countries, companies must respond to several requirements to ensure their cybersecurity is adequately protected. This may involve selecting protection tools based on the certification of compliance with information security requirements, having an information security system that includes storing personal information, and opting for other security measures selected based on the reliability and effectiveness of government systems or expenses. In this case, businesses need to go through the following steps to protect themselves through cybersecurity insurance:

[10] Verizon. (2020). 2020 Data Breach Investigations Report – Executive Summary. enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf

[11] Author's complied.

- Choose an insurance company that offers comprehensive cybersecurity protection services.
- Choose an expert organization to conduct information security audits (among organizations accredited by insurance companies).
- Assess and evaluate information security risks (conducted by an expert organization).
- Define the characteristics of security incidents.
- Determine the amount of insurance coverage and compensation for security incidents.
- Formulate a contract for comprehensive cybersecurity services.

Cybersecurity insurance policies (cyber liability insurance policies) are created as a means of protection against losses incurred as a result of cyberattacks and network breaches. They are designed to reduce losses incurred as a result of incidents such as cyberattacks and data breaches. Cybersecurity insurance is intended to cover losses resulting from cyberattacks and data breaches. This has arisen because existing insurance policies did not cover losses internally.

Table 3. Description of cyber insurance coverage [12]

Coverage Type	Description
Data Breach Coverage	Financial protection in the event of unauthorized access, disclosure, or theft of sensitive information, covering expenses such as notification, credit monitoring, and legal fees.
Cyber Extortion and Ransomware	Coverage for expenses incurred in response to ransomware attacks and extortion demands, including ransom payments, negotiation costs, and costs associated with data restoration.
Business Interruption	Compensation for income losses and extra expenses resulting from disruptions in operations caused by cyber incidents, helping businesses recover lost revenue and cover temporary costs.
Network Security Liability	Protection against third-party claims alleging damages resulting from a failure to safeguard sensitive information or prevent unauthorized access to networks or systems.
Regulatory and Legal Liability	Coverage for costs associated with regulatory investigations, fines, and legal proceedings resulting from non-compliance with data protection laws, privacy regulations, or industry standards.
Cyber Crime	Financial protection against losses resulting from various cybercrime activities, such as funds transfer fraud, social engineering scams, and identity theft.
Crisis Management	Access to crisis management and incident response services to effectively manage and respond to cyber incidents, including 24/7 incident response hotlines and forensic investigation assistance.
Risk Management Support	Resources and support to enhance cybersecurity posture and reduce exposure to cyber risks, such as cybersecurity assessments, employee training programs, and access to best practices.

Corporations benefit from cybersecurity in the following ways:

- Collection of Legal Payments: Legal payments resulting from cyberattacks, such as data breaches, can be quickly collected. In foreign countries, the maximum coverage

[12] Author's analysis.

amount offered by cybersecurity providers ranges from $1 million to $100 million for each claim.

- Recovery from Breaches: Cybersecurity helps in dealing with breaches by assisting in the dismissal of breaches that occur before the issuance of official government notifications.

- Compensation for Damages Resulting from Online Vandalism: In the event of cyber vandalism, cybersecurity assists businesses by covering damages, enabling security providers to compensate for lost funds.

Conclusion.

When it comes to managing cybersecurity risks, it's beneficial for both private enterprises and government organizations to reevaluate several key directions to assess the effectiveness of the arsenal of tools used for cyber defense:

Firstly, within the realm of management (related to business continuity and brand), recognizing and evaluating cyber risks, such as the threat of unauthorized access to a company's entry protection system by attackers, suppliers, and customers, is crucial. It's essential to identify resources, processes, and management tools to anticipate and identify cybersecurity incidents.

Secondly, the organizational and personnel aspect is crucial. To minimize cybersecurity threats, company leaders need to effectively collaborate with cybersecurity experts in every department to enhance their expertise in threats, attacks, and defense technologies. Effectively utilizing cybersecurity technologies and continuously updating them is crucial, particularly in the face of potential cyber threats.

Thirdly, based on these ideas, it may be suggested that cybersecurity is not only a technical issue for IT professionals but also involves human behavior. Therefore, mitigating risks through security measures is just as important as recognizing and managing them correctly. Company leaders need to understand these cybersecurity risks and how they should be managed. Employees and managers must be aware of how cybersecurity works and have the right to apply for security products that fit their risk profile to mitigate risks and minimize potential losses.

References.

1. Cebula, J.J. and Young, L.R. (2010) A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/ SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

2. Biener, Ch., & Eling, M & Wirfs, J. (2014). Insurability of Cyber Risk: An Empirical Analysis. Geneva Papers on Risk and Insurance - Issues and Practice. 40. 1-28. 10.1057/gpp.2014.19.

3. Böhme, Rainer & Kataria, Gaurav. (2018). Models and Measures for Correlation in Cyber-Insurance.

4. Ridd, J., 2002. Insuring Digital Risk: A Roadmap for Auction. Information Assurance Advisory Council. 28, 771-780

5. Hal Varian, Managing Online Security Risks, N.Y. Times, June 1, 2000.

6. Bodin, Lawrence & Gordon, Lawrence & Loeb, Martin & Wang, Aluna. (2018). Cybersecurity insurance and risk-sharing. Journal of Accounting and Public Policy. 37. 10.1016/j.jaccpubpol.2018.10.004.

7. Barreto, Carlos & Schwartz, Galina & Cardenas, Alvaro. (2021). Cyber-Insurance. 10.1007/978-3-030-65048-3_15.

8. https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

9. https://www.gartner.com/en/information-technology/insights/top-technology-trends
10. https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html
11. https://www.ibm.com/downloads/cas/ADLMYLAZ
12. Statista. (2021). Cyber insurance – Statistics & Facts. https://www.statista.com/topics/2445/cyber-insurance/
13. FBI. (2020). Internet Crime Report. ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
14. https://financesonline.com/cybersecurity-statistics/
15. RiskBased Security. (2020). 2020 Year End Report. pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf
16. Javelin. (2021). 2021 Identity Fraud Study: Shifting Angles. javelinstrategy.com/content/Javelin-2021-Identity-Fraud-Study
17. Verizon. (2020). 2020 Data Breach Investigations Report – Executive Summary. enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf