CYBER RISK MANAGEMENT AND THE ECONOMIC IMPACT OF DIGITAL SECURITY

CONCEPTUAL AND TECHNOLOGICAL PARTICULARITIES OF CYBER INSURANCE

UDC: 004.056.5:[368.022+368.03](100)
DOI: https://doi.org/10.53486/tids2025.07

IVAN LUCHIAN
Moldova State University
ivan.luchian@usm.md
ORCID ID: 0000-0002-8683-7228

SVETLANA GHERJAVCA
Moldova State University
svetlana.gherjavca@usm.md
ORCID ID: 0009-0002-2994-8412

Abstract. Cyber insurance (also called cyber liability insurance or cybersecurity insurance) encompasses insurance products designed to cover financial losses incurred by companies as a result of cyber incidents. These assurances are becoming increasingly important for all companies as the problems of cyber-attacks against applications, devices, networks, and users worsen, consequently requiring protection against cyber events, including acts of cyber terrorism, and can help remediate security incidents. This article aims to examine the specific characteristics of cyber insurance as a distinct financial product. The screening of open sources placed on the Internet was applied as a research method. Cyber insurance is an insurance product designed to protect corporate clients from risks related to information technology infrastructure and activities (such as data destruction, data extortion, theft, hacking, and denial-of-service attacks), as well as the liability of companies to third parties for damages caused, for example, by errors and omissions, failure to protect data, or defamation. Such insurance policies may also provide for regular security audits, post-incident public relations and investigation expenses, and criminal reward funds. The main areas that cyber insurance covers include: customer notifications; recovering personal identities; data breaches; data recovery; system damage repair; ransom demands; attack remediation; and liability for losses incurred by business partners with access to business data. Cyber insurance currently forms a continuously growing market segment of the global insurance market. This trend is maintained by the continuous development of the digital economy and e-commerce, the significant increase in the size of damages to companies following cyber incidents, as well as the permanent growth of technologies applied in cybercrime. At the same time, its size remains tiny compared to the global insurance market and the global cybersecurity market. Cyber insurance has a significant set of benefits. However, its spread is hindered by certain factors, the main ones being the specific conditions for the sale of insurance policies and the limits of insurance companies in assuming financial commitments.

Keywords: cyber insurance; liability; damage; security incident; cyber-attack.

JEL Classification: G22, L86

INTRODUCTION

Since the second half of the 1990s, the development of the digital economy and the information society has become a reality, and to this day, processes of deepening and development are taking place.

And as in any field of human activity, related malicious activities are simultaneously manifested, which affect the activity of companies in cyberspace.

In this context, Stocklytics experts (2024) state: "Despite the maximum efforts to prevent and minimize cybercrime damage, cyber-attacks, including ransomware attacks, data breaches, cyber espionage, phishing, and other espionage, are still the biggest threats in the business sector. According to the Allianz Risk Barometer survey, 40% of respondents called cybercrime their biggest potential threat in 2023, ahead of inflation, energy crises, and supply chain disruptions."

According to some estimates, 57% of business leaders believed that cyberattacks were inevitable (IBM, 2025).

In 2019, FM Global surveyed CFOs of companies with revenues of over $1 billion. It found that 71% of respondents said they believed their insurer would cover all or most of the potential losses in the event of a cyberattack (Granato, Polacek, 2019).

Therefore, modern companies, following the development of digital activities, have a growing need to ensure cybersecurity as a complex of methods and tools to protect systems, networks and programs from manifestations of cybercrime, which tend to alter, access or destroy sensitive information, extort users' funds, or disrupt normal economic activity (Fortune Business Insights, 2025).

One of the solutions aimed at strengthening the cybersecurity of companies is cyber insurance, which comes to supplement the cybersecurity system of corporate clients through a special insurance product.

Traditional insurance products for corporate clients, such as general liability and errors and omissions policies, typically do not cover losses caused by cyber incidents, leaving companies vulnerable to the full and significant cost of ransomware attacks, business email compromise scams, and other cybercrimes. For example, a ransomware attack costs an average of $4.54 million, not including ransom payments (IBM, 2025).

Cyber insurance policies are designed to fill this gap. By covering losses caused by cyber incidents, cyber insurance policies can help companies limit their damage, recover faster, and increase their overall level of cyber resilience (IBM, 2025).

The purpose of this article is to explain the essence of cyber insurance and present its technological particularities.

MAIN CONTENT

1. Materials and Methods

As a primary research method, screening of information available in various open publications on the Internet in the form of reports from specialized companies and views of experts in the field of cyber insurance was applied. Then the accumulated information was subjected to analysis and synthesis to obtain a complex picture of this specific insurance product.

2. Results and Discussion

The presentation of the results of the research begins with the definition of cyber insurance.

Cyber insurance (also known as cybersecurity insurance, cyber risk insurance, cyber liability insurance) is a specialty insurance product that allows companies to mitigate the consequences of the risk of cybercrime activities by covering the costs associated with data recovery after a cyber incident. This insurance product provides financial assistance and assistance in a cyber incident that could compromise private information, stop business activities, or cause financial damage (Fortinet), (IBM, 2025).

That is, it is a protection of corporate clients of insurance companies from dangers capable of affecting IT infrastructure, information governance, and information policy, which are not covered by traditional insurance policies. This insurance product works in the same way as if companies were to contract insurance against physical risks and natural disasters. Only the object of insurance differs (Fortinet).

The study identified the factors behind the increase in corporate customers' interest in cyber insurance.

First of all, it is about the rapid advancement of the process of developing the information economy, the expansion of electronic commerce, and the digitalization of companies' activities.

Secondly, there has been a rapid increase in corporate losses from cybercrime (Figure 1).

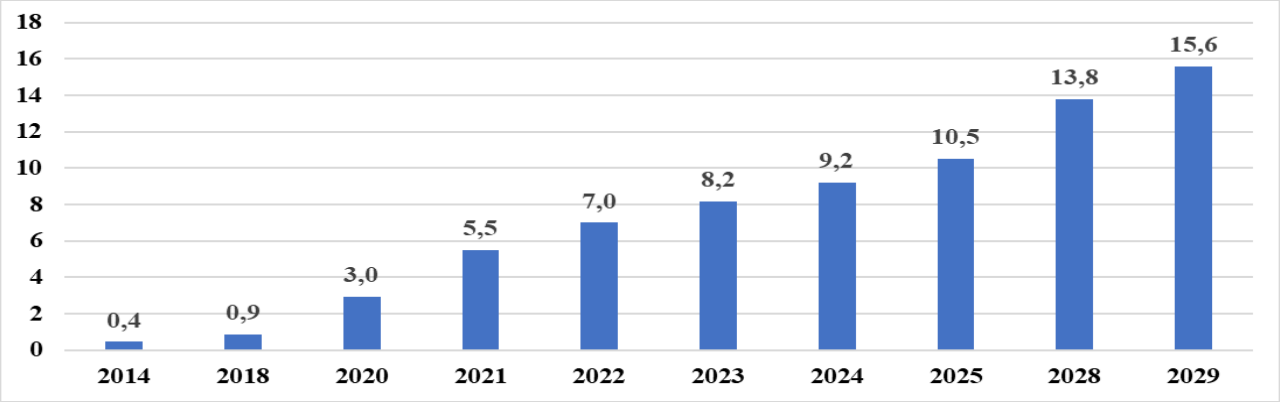

Figure 1. Dynamics of Global Cybercrime Costs (trillion U.S. dollars).
Sources: *(Fox, 2024), (Nakashima, Peterson, 2014), (Statista, 2024), (Stocklytics, 2024)*

Thus, if in 2014 the global costs of cybercrime amounted to about 445 billion US dollars, then for 2029 this indicator is estimated at 15.6 trillion US dollars.

IBM specialists (2025) report the following: “Security breaches are growing more common and more costly. According to IBM’s Cost of a Data Breach report, 83% of organizations have had more than one data breach, and the average breach costs USD 4.35 million. Cyber insurance can lessen the financial impact of these breaches, making it an important part of risk management for businesses today.”

Thirdly, it is essential to note the ongoing trend of cybercriminals continually improving their techniques to achieve their criminal objectives.

In the view of Embroker experts (2025), this insurance product is particularly advisable for certain industries that have an increased cyber risk: manufacturing, finance, insurance, energy and utilities, healthcare and pharmaceuticals, and technology.

On the other hand, considering that more and more companies are asking their employees to work from home and many companies are offering online services, it is very likely that social engineering attacks and data breach attempts will be on the rise for companies of all sizes and industries (Embroker, 2025).

The fourth factor is regulatory compliance requirements. Many countries have adopted robust regulatory frameworks to address cyber threats. In some jurisdictions, cyber insurance is mandatory, while in others, guidelines or incentives have been implemented for companies to obtain such coverage voluntarily (LAMDA Broking, 2023).

For example, in some countries, legislation requires companies that have contracts that have access to sensitive government data to have cyber insurance (Abacus).

Under the impact of these factors, the value of the cyber insurance market has grown rapidly (Table 1).

Generalizing the data in the table, we can conclude that in 2024 the average size of the cyber market was 15.6 billion US dollars, slightly exceeding the level of 2023 (15.3 billion US dollars), and for 2025, an increase to 16.3 billion US dollars is expected. For the next ten years, a CAGR level of 18.4% is likely.

Table 1. The current and prospective global cybersecurity market size.

Expert company	Market size (billion US dollars)						CAGR (%)
	2023	2024	2025	2032	2033	2034	
Imarc Group		**14,2**			**73,5**		**17,9**
Fortune Business Insights	**16,7**	**20,9**		**120,5**			**24,5**
Skyquestt	**14,0**	**16,8**		**71,8**			**19,9**
Insight Ace Analytic		**11,0**				**32,3**	**11,5**
Munich Re		**15,3**	**16,3**				

Sources: *(Fortune Business Insights, 2025), (Imarc Group, 2024), (Insight Ace Analytic, 2025), (Munich Re, 2025), (Skyquestt, 2025)*

Geographically, North America accounted for 36.61% of the market share in 2023. (Fortune Business Insights, 2025)

The total volume of premiums collected in the global cyber insurance market in 2023 amounted to 14 billion US dollars, increasing to 15.3 billion US dollars in 2024. For the future, an increase of up to 29 billion US dollars is forecasted by 2027 (Cobalt, 2024), (Munich Re, 2025).

In 2024, North America earned $10.6 billion in premiums, accounting for 69% of global premiums. And premiums earned in Europe were $3.3 billion, accounting for 21% of global premiums (Munich Re, 2025).

Despite the fact that cyber insurance is a rapidly growing business, it is still a relatively small part of the insurance market. For example, according to data provided by Swiss Re (2024), the size of the global insurance market was 3.1 trillion US dollars, which means that the share of the global cyber insurance market in the global insurance market is 0.49%. And the global cybersecurity market is 193.7 billion US dollars (Fortune Business Insights, 2025).

According to data provided by Embroker (2025), in 2024, the average payment amount of a company for cyber insurance was between 1,200 and 7,000 US dollars annually, with an average cost of approximately 2,000 US dollars per year. And the limits of cyber liability coverage are between 500 thousand US Dollars and 5 million US Dollars per insurance case.

The following variables can be mentioned as variables taken into account: company size, industry, amount and sensitivity of data, annual revenue, strength of security measures, and cyber liability coverage limits, claims history (Embroker, 2025).

The history of cyber insurance began in 1997, when insurance policies were intended for information technology companies responsible for managing networks and systems used by other companies and consumers (Granato, Polacek, 2019).

In the early 2000s, online media insurance policies began to cover unauthorized access, network security, data loss, and damage related to computer worms or viruses (Prowriters).

Cyber insurance policies also did not include both direct and third-party coverage at the same time. It was not until the mid-2000s that these policies, in response to cyber threats, included some direct coverage to protect companies themselves and potentially intellectual property. New policies included coverage for cyber business interruption, cyber extortion, and damage to network assets.

In 2003, the California Information and Security Breach Act, which affected both exposure and cyber insurance, went into effect. Companies operating in the state were required to provide notice to any affected residents of a personal data breach by an unauthorized party. Many other states then passed similar laws. Cyber insurance companies quickly adjusted their offerings with direct coverages such as IT forensics and information security, public relations, credit monitoring, and customer notification. New coverages were also developed for third-party, regulated defense, and fines and penalties that could be tied to notification of affected parties.

To the present moment, the examined market has widened, and three forms of cyber protection through insurance can be identified at the moment:

- Third-party coverage;
- First-party coverage;
- Silent cyber coverage.

Third-party cyber insurance (third-party cyber liability insurance) is designed to provide liability coverage for companies responsible for a client's online security. That is, it is liability coverage for companies responsible for the online security and data of their clients, but who fail to prevent a data breach or cyberattack on a client. For example, if an IT company's client suffers a ransomware attack or data breach and sues the IT company, third-party cyber insurance can cover the necessary legal expenses (Insureon), (TechInsurance).

First-party cyber insurance is intended to directly cover the policyholder from the financial consequences of cybersecurity breaches in a company's own network (Coalition), (Insureon).

Silent cyber (also known as unintended or non-affirmative) coverage provides coverage for unknown (or unquantified) exposures arising from cyber hazards that may be triggered under traditional property and liability insurance policies (GuyCarpetenter).

Cyber insurance policies usually offer the following (*5 Types…,* n.d.):

1. Privacy liability coverage. It is important for companies that handle sensitive employee and customer information. It helps protect the company in the event of a data breach that exposes private data and exposes the company to liability. This coverage protects against liabilities resulting from breaches of privacy law or cyber incidents involving private data. These events often result in third-party liability costs due to contractual obligations or regulatory investigations.

2. Network security. This protects a company during network security failures such as data breaches, cyber extortion requests, malware infections, business email compromise events, and ransomware. This covers direct costs incurred by the first party as a result of a cyber incident, including IT forensic investigations, legal fees, data restoration, ransomware negotiation and payment, consumer notification of the security breach, public relations expenses, call center setup, credit monitoring, and identity restoration.

3. Network business interruption. Network business interruption insurance helps companies exposed to operational cyber risk. This includes losses resulting from system failures (such as human error or a failed software patch) and security failures (such as a third-party cyber-attack).

4. Errors and omissions (E&O) coverage. In this case, it is about protecting companies from cyber incidents that prevent the provision of services to customers and the execution of contractual obligations. This includes claims of errors or performance failures in services, such as software and consulting services, as well as professional services. Errors and omissions coverage refers to allegations of negligence or breaches of contract, covering legal defense costs incurred due to lawsuits or disputes with customers.

5. Media liability coverage. This insurance is designed to protect companies from intellectual property damage, excluding patent infringement. It is typically used in print and online advertising, including company posts on social media.

A cybersecurity insurance policy will often exclude issues that were caused by human error or negligence or could have been prevented, such as (*5 Types…,* n.d.), (Fortinet):

- *Poor security processes:* cyber-attacks become possible due to security gaps or ineffective configuration management.
- *Prior breaches:* these are security incidents that occurred before the company purchased a cyber insurance policy.
- *Human error:* these are cyberattacks caused by human errors committed by company employees.
- *Insider attacks:* data loss or theft caused by an internal attack, which made a company employee vulnerable.
- *Pre-existing vulnerabilities:* this is the case when a company suffers a data breach as a result of not addressing or remediating previously known vulnerabilities.
- *Technology system improvements:* this includes any costs related to technological improvements, such as network and application improvements.

Expert Dan Burke (2025) presented the new trends in cyber risk management in 2025:

- *Technology supply chain attacks*. Given that some companies take a relatively long time to patch known vulnerabilities, attackers can exploit these vulnerabilities as long as they exist, generating losses for companies with cyber insurance.
- *Securities and Exchange Commission (SEC) enforcement*. Recent SEC decisions in the United States point to a less risky regulatory environment regarding cybersecurity for public companies and their Chief Information Security Officers. The SEC recently launched the Cyber and Emerging Technologies Unit (CETU) to address cybersecurity misconduct and protect individual investors from malicious cyber actors. The CETU will focus on the following priority areas: fraud committed using emerging technologies, such as artificial intelligence and machine learning; use of social media, the dark web, or false websites to perpetrate fraud; hacking to obtain material nonpublic information; takeovers of retail brokerage accounts; fraud involving blockchain technology and crypto assets; regulated entities' compliance with cybersecurity rules and regulations; public issuer fraudulent disclosure relating to cybersecurity (SEC, 2025).
- *Artificial intelligence (AI) risk*: The adoption of artificial intelligence is accelerating rapidly, and many of the risks associated with it have yet to be discovered. When there is such uncertainty, an insurance policy can help a company leverage the power of artificial intelligence without taking on too much risk. Likewise, many experts warn about the use of AI to carry out cybercrime.
- *Non-breach privacy claims.* Legal issues related to litigation under US privacy laws, particularly the Video Privacy Protection Act (VPPA), highlight the need for companies to improve their data practices and ensure they obtain explicit consent from users before sharing any personal information.

CONCLUSIONS

Cyber insurance is a special insurance product designed to limit the liability of a corporate policyholder and help manage recovery costs in the event of a cyber incident.

Cyber insurance helps protect companies against security risks, the diversity of which increases year by year. And threats to companies' cybersecurity are constantly evolving.

It is a complex product made up of three basic components: third-party coverage, first-party coverage, and silent cyber coverage.

At present, we can speak of the existence of a global cyber insurance market, the essential part of which is located in the US. Although its share is relatively modest within the global insurance market, the dynamics of its expansion are impressive.

REFERENCES

1. *5 Types of Cyber Security Insurance Coverage and what to watch out for*. Available at: https://www.bluevoyant.com/knowledge-center/5-types-of-cyber-insurance-coverage-and-what-to-watch-out-for [Accessed 08.05.2025]
2. Abacus. *How Cyber Insurance Plays A Role in Risk Management and Regulatory Compliance*. Available at: https://goabacus.com/how-cyber-insurance-plays-a-role-in-risk-management-and-regulatory-compliance/ [Accessed 10.05.2025]
3. ABI. What does cyber insurance cover?. Available at: https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/cyber-insurance/what-does-cyber-insurance-cover/ [Accessed 10.05.2025]
4. Burke Dan, 2025. *Cyber Insurance in 2025: What to Expect*. Available at: https://woodruffsawyer.com/insights/cyber-looking-ahead-guide [Accessed 17.05.2025]
5. Cobalt, 2024. *Top Cybersecurity Statistics for 2025*. Available at: https://www.cobalt.io/blog/top-cybersecurity-statistics-2025 [Accessed 10.05.2025]
6. Embroker, 2025. *How much does cyber insurance cost in 2025?*. Available at: https://www.embroker.com/blog/cyber-insurance-cost/ [Accessed 12.05.2025]
7. Fortinet. *What Is Cyber Insurance? Why Is It Important?*. Available at: https://www.fortinet.com/resources/cyberglossary/cyber-insurance Accessed 12.05.2025]
8. Fortune Business Insights, 2025. *Cyber Insurance Market Size, Share & Industry Trends Analysis, By Insurance Type (Standalone and Tailored), By Coverage Type (First-party and Liability Coverage), By Enterprise Size (SMEs and Large Enterprise), By End-user (Healthcare, Retail, BFSI, IT & Telecom, Manufacturing, and Others), and Regional Forecast, 2024-2032*. Available at: https://www.fortunebusinessinsights.com/cyber-insurance-market-106287 [Accessed 09.04.2025]
9. Fortune Business Insights (2025) *Cybersecurity Market Size, Share & Industry Analysis, By Component (Solutions and Services), By Deployment (On-premises and Cloud), By Security Type (Network Security, Cloud Application Security, End-point Security, Secure Web Gateway, Application Security, and Others), By Enterprise Size (Small & Medium Enterprises (SMEs) and Large Enterprises), By Industry (BFSI, IT and Telecommunications, Retail, Healthcare, Government, Manufacturing, Travel and Transportation, Energy and Utilities, and Others), and Region Forecast, 2024-2032*. Available at: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165 [Accessed 09.04.2025]
10. Fox Jacob (2024). *Top Cybersecurity Statistics for 2025*. Available at: https://www.cobalt.io/blog/top-cybersecurity-statistics-2025 [Accessed 05.05.2025]
11. Granato Andrew, Polacek Andy, 2019. *The Growth and Challenges of Cyber Insurance*. Available at: https://www.chicagofed.org/publications/chicago-fed-letter/2019/426#:~:text=In%20July%202019%2C%20FM%20Global,would%20suffer%20in%20a%20cyberattack. [Accessed 16.05.2025]

12. GuyCarpetenter. *Affirmative versus silent syber: an overview*. Available at: https://www.guycarp.com/insights/2018/11/affirmative-versus-silent-cyber-an-overview.html#:~:text=Non%2Daffirmative%2Fsilent%2Funintended,every%20type%20of%20insurance%20policy [Accessed 06.05.2025]
13. IBM (2025). *What is cyber insurance?*. Available at: https://www.ibm.com/think/topics/cyber-insurance [Accessed 09.04.2025]
14. Imarc Group (2024) *Cyber Insurance Market Size, Share, Trends and Forecast by Component, Insurance Type, Organization Size, End Use Industry, and Region, 2025-2033*. Available at: https://www.imarcgroup.com/cyber-insurance-market [Accessed 03.05.2025]
15. Insight Ace Analytic (2025) *Cyber Insurance Market Research Report*. Available at: https://www.insightaceanalytic.com/report/cyber-insurance-market/1634 [Accessed 03.05.2025]
16. Insureon. *Third-party cyber insurance coverage*. Available at: https://www.insureon.com/small-business-insurance/cyber-liability/third-party [Accessed 16.05.2025]
17. LAMDA Broking, 2023. *Cyber Insurance and Regulatory Compliance: Safeguarding Data in a Global Context*. Available at: https://www.linkedin.com/pulse/cyber-insurance-regulatory-compliance [Accessed 03.05.2025]
18. Markets and Markets (2024) *Cybersecurity market size, share, industry, overview, growth, latest trends*. Available at: https://www.marketsandmarkets.com/market-reports/cyber-security-market-505.html#:~:text=the%20global%20cybersecurity%20market%20size,projected%20to%20reach%20%24298.5%20billion [Accessed 02.05.2025]
19. Munich Re (2025) *Cyber Insurance. Risks and Trends 2025*. Available at: https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html#:~:text=Cyber%20insurance%20market%20trends,the%20insurance%20industry%20going%20forward [Accessed 02.05.2025]
20. Nakashima Ellen, Peterson Andrea (2014) *Report: Cybercrime and espionage costs $445 billion annually*. Available at: https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html [Accessed 02.05.2025]
21. Prowriters. *Cyber Insurance Blog*. Available at: https://prowritersins.com/cyber-insurance-blog/history-cyber-insurance/ [Accessed 17.05.2025]
22. Securities and Exchange Commission, 2025. *SEC Announces Cyber and Emerging Technologies Unit to Protect Retail Investors*. Available at: https://www.sec.gov/newsroom/press-releases/2025-42 [Accessed 17.05.2025]
23. Silverfort. *Cyber Insurance*. Available at: https://www.silverfort.com/glossary/cyber-insurance/ [Accessed 08.04.2025]
24. Statista (2024) *Annual cost of cybercrime worldwide 2018-2029*. Available at: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide [Accessed 05.05.2025]
25. Stocklytics (2024) *Annual Cybercrime Cost to Jump by 70% and hit $13.8 Trillion by 2028*. Available at: https://www.globalsecuritymag.com/annual-cybercrime-cost-to-jump-by-70-and-hit-13-8-trillion-by-2028.html [Accessed 05.05.2025]
26. Skyquestt (2025) *Cyber Insurance Market Size, Share and Growth Analysis*. Available at: https://www.skyquestt.com/report/cyber-insurance-market [Accessed 03.05.2025]
27. Swiss Re, 2024. sigma 5/2024: Global economic and insurance market outlook 2025-26. Available at: https://www.swissre.com/institute/research/sigma-research/sigma-2024-05-global-economic-insurance-outlook-growth-geopolitics.html [Accessed 07.05.2025]
28. TechInsurance. *Third-party cyber liability insurance*. Available at: https://www.techinsurance.com/insurance-terms/third-party-cyber-liability [Accessed 16.05.2025]
29. Wikipedia. *Cyber insurance*. Available at: https://en.wikipedia.org/wiki/Cyber_insurance [Accessed 08.05.2025]