DOI: 10.31379/sed.1.4.2025.38
UDK 658.5:004.8:330.341.1

LAKHTIONOVA Anastasiia
Senior financial officer
Marine Technology Department
Norwegian University of Science and Technology,
Trondheim, Norway
ORCID: 0009-0002-4154-2263
E-mail:
anastasiia.lakhtionova@gmail.com

GLOBAL CYBERSECURITY MARKET 2017–2029: DYNAMICS, STRUCTURE, CHALLENGES AND KEY PLAYERS

Abstract
The article provides a comprehensive analysis of the global cybersecurity market for the period 2017–2029 based on data from Statista Market Insights' Cybersecurity Market Report (2024). It is found that the market volume will grow from US$89.72 billion in 2017 to a projected US$271.90 billion in 2029, corresponding to a compound annual growth rate (CAGR) of 9.68%. The market is divided into two main segments: Security Services ($155.7 billion in 2024, 52.4% of the total volume) and Cyber Solutions ($88.4 billion). A regional comparison of five key countries (US, China, UK, Japan, Germany), which together generate 66.8% of the industry's global revenues, is made. The most dynamic national market is China (CAGR 12.7%); the absolute leader is the USA (65.6% of the top five). The structure of cyber threats is analyzed, where phishing schemes account for 53.24% of all attacks, and the average cost of a data breach in the healthcare industry exceeds the global average by 2.46 times. Special attention is paid to the corporate strategies of industry leaders - Microsoft Corporation (CAGR 14% in 2020–2023) and IBM (CAGR 3.9%). The basic, optimistic and pessimistic scenarios for the development of the industry until 2030 are formulated.

Keywords: cybersecurity, cybersecurity market, Security Services, Cyber Solutions, cyber threats, data breaches, phishing, IT budgets, digital transformation, CAGR, Microsoft, IBM.

JEL Classification: M31, M37, C12, L82

Received: 24/02/2025
Accepted:25/03/2025
Published:28/04/2025

© Copyright 2025by the author(s)
This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

ГЛОБАЛЬНИЙ РИНОК КІБЕРБЕЗПЕКИ 2017–2029: ДИНАМІКА, СТРУКТУРА, ВИКЛИКИ ТА КЛЮЧОВІ ГРАВЦІ

ЛАХТІОНОВА Анастасія
Фінансовий консультант у сфері проектної економіки
Кафедра морських технологій
Норвезький науковий технічний університет
Трондхейм, Norway
ORCID: : 0009-0002-4154-2263
e-mail:
anastasiia.lakhtionova@gmail.com

Анотація
У статті здійснено комплексний аналіз глобального ринку кібербезпеки за період 2017–2029 років на основі даних звіту

Statista Market Insights «Cybersecurity Market Report» (2024). Виявлено, що обсяг ринку зросте з 89,72 млрд доларів США у 2017 році до прогнозованих 271,90 млрд у 2029 році, що відповідає середньорічному темпу приросту (CAGR) 9,68%. Ринок поділяється на два основні сегменти — Security Services (155,7 млрд дол. у 2024 р., 52,4% сукупного обсягу) та Cyber Solutions (88,4 млрд дол.). Здійснено регіональне порівняння п'яти ключових країн (США, Китай, Велика Британія, Японія, Німеччина), які сукупно генерують 66,8% глобальних доходів галузі. Найбільш динамічним національним ринком є Китай (CAGR 12,7%); абсолютним лідером — США (65,6% від обсягу п'ятірки). Проаналізовано структуру кіберзагроз, де phishing-схеми становлять 53,24% усіх атак, а середня вартість витоку даних у галузі охорони здоров'я перевищує глобальне середнє у 2,46 рази. Окрему увагу приділено корпоративним стратегіям лідерів галузі — Microsoft Corporation (CAGR 14% у 2020–2023 рр.) та IBM (CAGR 3,9%). Сформульовано базовий, оптимістичний та песимістичний сценарії розвитку галузі до 2030 року.

Подано: 24/02/2025
Прийнято:25/03/2025
Опубліковано:28/04/2025

© Copyright 2025by the author(s)
This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

Ключові слова: кібербезпека, ринок кібербезпеки, Security Services, Cyber Solutions, кіберзагрози, витоки даних, phishing, IT-бюджети, цифрова трансформація, CAGR, Microsoft, IBM.

JEL Classification: M31, M37, C12, L82

Introduction

Cybersecurity has become one of the most dynamic and strategically important issues of the modern digital economy. Until recently, it was considered mainly a technical competence of the IT department, but in the mid-2020s, it became a fundamental component of corporate strategy, state national security policy, and geopolitical competition. No organization — from small startups to multinational corporations and governments — can function successfully without a systematic approach to protecting information assets from malicious actions.

The relevance of the chosen research topic stems from several interrelated factors. First, the rapid development of the global cybersecurity market — according to forecasts, from 89.72 billion US dollars in 2017 to 271.90 billion in 2029 — is driving the formation of a mega-industry, making it one of the leading segments of the IT industry. Second, the 2020–2022 COVID-19 pandemic and the full-scale Russian-Ukrainian war that began in February 2022 have fundamentally transformed the digital threat landscape: the massive shift of organizations to remote work, the accelerated migration to cloud infrastructures, and the use of digital technologies in the military have created a fundamentally new level of both opportunities and risks. Third, the emergence of generative artificial intelligence and quantum computing in the medium term poses fundamentally new methodological challenges for the industry, both in defense and in attack. Ukraine occupies a special place in the modern global cybersecurity landscape. First, since 2014, the domestic digital infrastructure has become the first in modern history to serve as the testing ground for massive state cyber operations (in particular, the NotPetya attacks of 2017, a series of attacks on the energy system in 2015–2016, and continuous cyber campaigns after February 24, 2022). Second, Ukraine's successful experience in repelling Russian cyber aggression has transformed domestic specialists into among the most experienced in the world — an important strategic asset for post-war

DOI: 10.31379/sed.1.4.2025.38

recovery and integration into the European digital space. Third, the formation of a national cyber strategy and regulatory framework (in particular, the Law "On the Basic Principles of Ensuring Cybersecurity of Ukraine" of 2017) lays the foundation for a full-fledged national cybersecurity ecosystem.

Literature review

The term "cybersecurity" has several related, though not identical, definitions in the scientific and regulatory literature. The classic technical definition adopted by the US National Institute of Standards and Technology (NIST) describes cybersecurity as the ability to protect or defend cyberspace against cyberattacks. The European Network and Information Security Agency (ENISA) offers a broader formulation: cybersecurity is the set of activities, resources, skills, processes, best practices, assurance mechanisms,, and technologies used to protect cyberspace, its users, and affected individuals from cyber threats.

In Ukrainian legislation, the definition is given in the Law "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017): "cybersecurity is the protection of the vital interests of a person and a citizen, society and the state when using cyberspace, which ensures the sustainable development of the information society and the digital communication environment, the timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace". This definition is particularly notable for combining the technical, social, and national security dimensions of the phenomenon. In academic economic literature, cybersecurity is increasingly viewed not only as a technological function, but also as a specific market phenomenon with its own supply and demand structure, pricing, competitive environment, and innovation cycle. It is this economic approach that underpins our research. In the business dimension, the cybersecurity market comprises organizations that offer specialized products and services to protect digital assets from unauthorized access, damage, theft, or other malicious activities. It is critically important to realize that cybersecurity today is not an optional aspect of digital activity, but a necessary prerequisite for its success. In a rapidly digitalized economy, companies that ignore or underinvest in cybersecurity risk are experiencing critical financial and reputational losses: according to the IBM Cost of a Data Breach Report 2023, the average cost of a data breach on a global scale reached $4.45 million, and in certain industries (healthcare), over $10.93 million.

1.2. Cybersecurity Market Structure: Segmentation

Statista Market Insights' Cybersecurity Market Report (2024) divides the cybersecurity market into two major segments, reflecting different security implementation models:

The first segment — Security Services — covers services provided by specialized companies to enhance organizations' security and defense strategies. It includes: cybersecurity consulting, information systems auditing, penetration testing, Security Operations Center (SOC) services, incident response, staff training, and legal and compliance support. This segment is larger in volume and, as of 2024, is 97.30 billion US dollars, or 52.4% of the total market.

The second segment - Cyber Solutions — combines automated technological solutions aimed at protecting against cyberattack risks: antivirus software, firewalls, intrusion detection and prevention systems (IDS/IPS), endpoint protection solutions (EDR/XDR), identity and access management systems (IAM), cloud infrastructure protection (CASB, CSPM), Zero Trust Architecture solutions, data encryption, backup, and disaster recovery. The volume of this segment in 2024 is 88.39 billion US dollars, or 47.6% of the market.

The structural ratio between these segments is gradually changing: if in 2017 Security Services accounted for 62.4% of the total volume (56.01 out of 89.72 billion), then in 2029 their share is predicted to decrease to 45.5% (123.60 out of 271.90 billion). This indicates a faster growth rate for the Cyber Solutions segment, which aligns with the broader trend of cybersecurity automation through AI, machine learning, and security orchestration (SOAR).

DOI: 10.31379/sed.1.4.2025.38

In addition to this basic segmentation, the cybersecurity market can be structured by: types of customers (corporate vs. government vs. small and medium-sized businesses vs. B2C); industry specifics (financial services, healthcare, energy, manufacturing); geographical characteristics (national and regional markets); types of threats addressed by the solutions (protection against ransomware, DDoS, phishing, APT, etc.).

Aims and Objectives

The purpose of the article is to conduct a comprehensive analysis of the global cybersecurity market for the period 2017–2029, identify the patterns of its development, identify key driving forces, assess the structure of threats and costs, characterize the positions of leading corporate players, and formulate reasonable forecasts for the development of the industry by the end of the decade.

To achieve this goal, the following tasks are solved in the work:

• to systematize theoretical and methodological approaches to defining cybersecurity as an economic category and market segment;

• to analyze the dynamics of the volume of the global cybersecurity market for 2017–2029 with a decomposition into the Security Services and Cyber Solutions segments;

• to calculate the growth rates, CAGR and structural parameters of the market;

• to conduct a comparative analysis of five key national markets (USA, China, Great Britain, Japan, Germany);

• identify macroeconomic, technological, and behavioral drivers of industry development;

• investigate the structure of cyber threats and data breach costs by industry;

• characterize the financial indicators and strategies of key corporate players;

• formulate a scenario forecast for the industry development until 2030.

The study focuses on the global cybersecurity market as a segment of the digital economy. The study examines the quantitative parameters of the market, including its structure, functioning, patterns, and development trends.

The scientific novelty of the work lies in the comprehensive systematization of the latest data on the state of the global cybersecurity market, in the proposed approach to comparing the dynamics of the Security Services and Cyber Solutions segments, in calculating structural coefficients of regional concentration, as well as in formulating scenario forecasts taking into account the specific context of the Russian-Ukrainian war as a global driver of demand for cybersecurity services.

Methods

The study's information base is characterized by several methodological features. First, Statista Market Insights data is based on its own market assessment models that combine top-down (macroanalytical) and bottom-up (aggregation of corporate data) approaches. This allows for consistent market assessments even in conditions of fragmented primary reporting.

Second, the forecast values for 2025–2029 are based on linear and regression models that use historical trends, adjusted for expected macroeconomic and technological factors. Like any forecasts, they carry uncertainty that increases over long periods.

Thirdly, data on corporate indicators (Microsoft, IBM) are sourced from official financial statements in the appropriate formats (10-K Annual Reports), ensuring their high reliability.

The following methods were used in the study: 1) time series analysis - to identify long-term trends; 2) calculation of CAGR according to the formula CAGR = (V_end/V_start)^(1/n) − 1 - for an aggregate assessment of growth rates; 3) method of absolute and relative values - to characterize volumes; 4) method of comparative analysis - to compare national markets and segments; 5) method of structural coefficients - to assess market concentration; 6) graphical method - to visualize trends; 7) scenario modeling - for forecasting.

DOI: 10.31379/sed.1.4.2025.38

The information base of the study was the data of the Statista Market Insights report "Cybersecurity Market Report" (2024), based on Statista's own market assessment models, supplemented by data from the IBM Cost of a Data Breach Report 2023, NordVPN, Flexera 2023 State of Tech Spend Report, and annual reports of Microsoft (Annual Report 2023) and IBM (Annual Report 2023). The methodological basis comprises methods of economic and statistical analysis of time series, the calculation of average annual growth rates (CAGR) using the compound interest formula, the comparative analysis method, and the graphical modeling.

Results

Analysis of the dynamics of the global cybersecurity market over the thirteen-year period 2017–2029 allows us to identify a fundamental trend - a steady, progressive growth in the market volume without a single year of decline. This phenomenon is especially notable against the background of the fact that during the period under study the industry went through several significant macroeconomic shocks: the COVID-19 pandemic (2020–2022), the supply chain crisis, the inflation wave of 2022–2023, the full-scale Russian-Ukrainian war (since 2022). None of these shocks caused a drop in demand for cybersecurity services - on the contrary, in many cases they became an additional factor in accelerating growth. The quantitative dynamics of the market are clearly presented in Figure 2.1, which contains a breakdown of the industry's total revenues into two main segments - Security Services and Cyber Solutions.

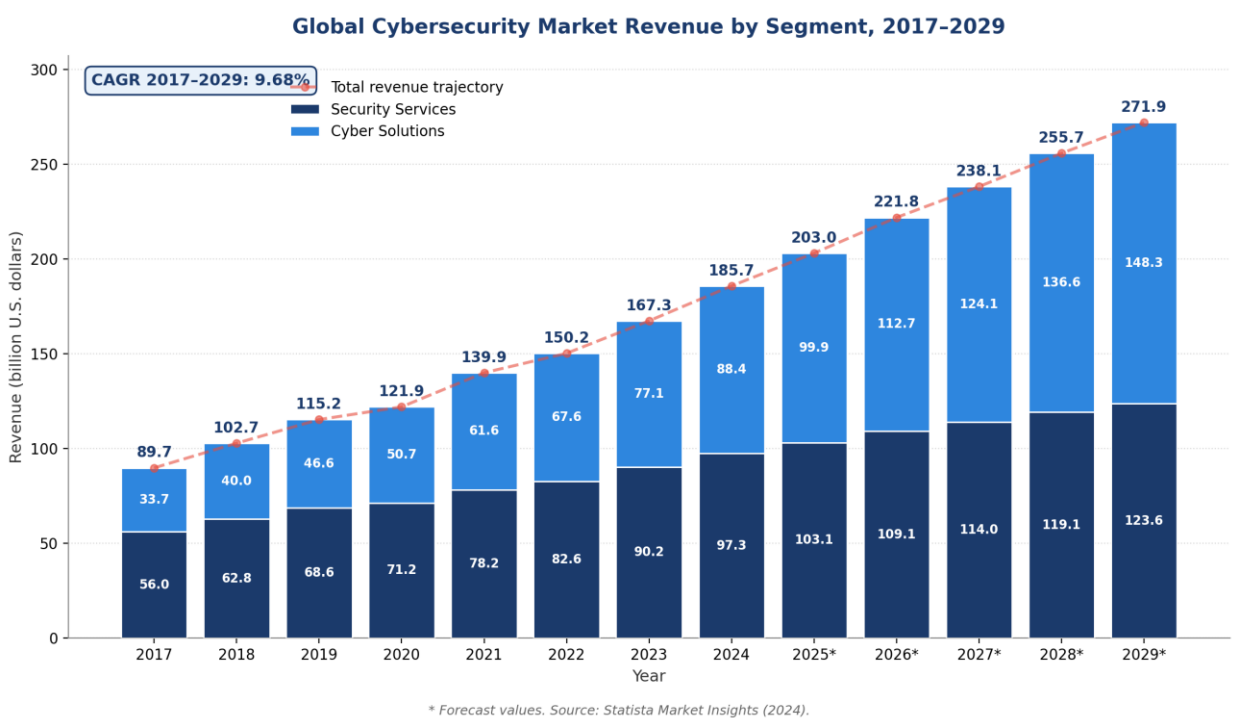


Figure 1 — Dynamics of the global cybersecurity market by segment, 2017–2029, billion USD
Source: constructed by the author based on data from Statista Market Insights (2024).

As shown in the figure, the market volume will grow from 89.72 billion US dollars in 2017 to 271.90 billion in 2029. The total growth over thirteen years is about 203%, or 3.03 times. The average annual growth rate (CAGR) for the period 2017–2029 is 9.68%, which corresponds to the market's characteristic of steadily growing with moderate but steady rates. For comparison, the average annual growth rates of global GDP over the same period fluctuated mainly between 2.5–3.5%, and the IT services market in general, about 6–8%. That is, cybersecurity grew much faster than the general economy and noticeably faster than its parent

DOI: 10.31379/sed.1.4.2025.38

sector.

A special feature of the dynamics is the absence of so-called “bubble” episodes. Unlike many other segments of the digital economy (including Web 3.0, metaverses, and generative AI), which experience periods of sharp excitement followed by corrections, the cybersecurity market shows almost linear growth. This indicates a fundamental, rather than opportunistic, nature of demand: organizations do not “buy” cybersecurity as a fashionable trend, but invest in it as a necessary operational function.

Table 1 summarizes the key parameters of market dynamics by selected sub-periods - this is our first calculation table.

Table 1 — Estimated parameters of the dynamics of the global cybersecurity market by sub-periods

Sub-period	Beginning (billion dollars)	End (billion USD)	Abs. growth	Rel. growth, %	CAGR, %
I. 2017–2019 (pre-pandemic)	89,72	115,21	25,49	28,41	13,33
II. 2020–2022 (pandemic/corrective)	121,92	150,16	28,24	23,16	10,98
III. 2023–2024 (post-crisis)	167,29	185,69	18,40	11,00	11,00
IV. 2025–2029 (forecast)	202,99	271,90	68,91	33,95	6,02
The entire period 2017–2029	89,72	271,90	182,18	203,06	9,68

Source: calculated by the author based on data from Statista Market Insights (2024).

Analysis of the data presented in Table 1 reveals an interesting pattern: the highest growth rates were observed in the pre-pandemic period of 2017–2019 (CAGR 13.33%), which is explained by the “low base” of comparison and active market formation. The pandemic period saw a slight slowdown in rates (10.98%), but absolute volumes continued to grow. The forecast period of 2025–2029 predicts a further slowdown in relative rates to 6.02% — a typical trajectory for a market entering maturity. At the same time, the forecast period's absolute growth ($68.91 billion) exceeds the total growth across all previous sub-periods ($72.13 billion) by only 4.5%, demonstrating that, while maintaining gradual rates, absolute volumes are becoming increasingly significant.

The decomposition of the market into two main segments allows us to see one of the most significant structural trends in the industry - a gradual shift in the ratio in favor of Cyber Solutions. In 2017, the Security Services segment accounted for 62.43% of the total market volume (56.01 billion out of 89.72 billion), and Cyber Solutions - 37.57% (33.71 billion). By 2024, the shares were balanced: 52.40% (97.30 billion) accounted for Security Services and 47.60% (88.39 billion) - for Cyber Solutions. According to the forecast for 2029, the situation will reverse: Cyber Solutions will account for 54.54% (148.30 billion), and Security Services 45.46% (123.60 billion).

This structural shift has several important consequences. First, Cyber Solutions’ growth in share indicates the progressive automation of cybersecurity: organizations are increasingly relying on technological solutions rather than outsourcing. Second, this shift reflects the shortage of qualified cybersecurity professionals in the labor market - the shortage of human resources is forcing companies to look for solutions in the form of AI tools and automation. Third, the growth rate of Cyber Solutions (CAGR of 12.9% in 2017-2029) significantly exceeds that of Security Services (6.8% over the same period), reflecting a faster innovation cycle in the technology segment. A more detailed analysis of the dynamics of chain growth rates allows us to identify several key events that have influenced the market. Thus, the highest chain growth (12.12%) occurred in 2019 (from 102.74 to 115.21 billion) — a period of active industry

DOI: 10.31379/sed.1.4.2025.38

formation, when SOC services and cloud solutions were just gaining popularity. In 2020, the pace slowed down to 5.82% — a consequence of the pandemic shock, which temporarily disrupted business cycles. However, in 2021, the pace sharply accelerated to 14.73% - the highest value for the entire observed period — driven by the massive transition of organizations to remote work and a sharp increase in the need to protect the digital perimeter. In 2022, the growth rate decreased to 7.34% - partly due to a high comparison base and partly due to macroeconomic turmoil (rate increases, reductions in IT budgets). However, in 2023, the market received a new powerful impetus - the full-scale Russian-Ukrainian war, which became the catalyst for massive cyber campaigns against European and North American infrastructure, increasing awareness of the criticality of cybersecurity. The growth rate in 2023 was 11.41%, and in 2024, 11.00%.

The forecast rates for 2025–2029 provide for a gradual slowdown from 9.32% in 2025 to 6.38% in 2029. This reflects the natural process of market "maturation", when rapid growth is replaced by stable development. However, even the forecast rates of 6–9% remain higher than the expected growth rates of the global economy, indicating the continued outpacing of cybersecurity development compared to the rest of the segments.

The global cybersecurity market is characterized by significant geographical concentration. Figure 2 presents a comparative description of five key national markets: the United States, China, the United Kingdom, Japan, and Germany.

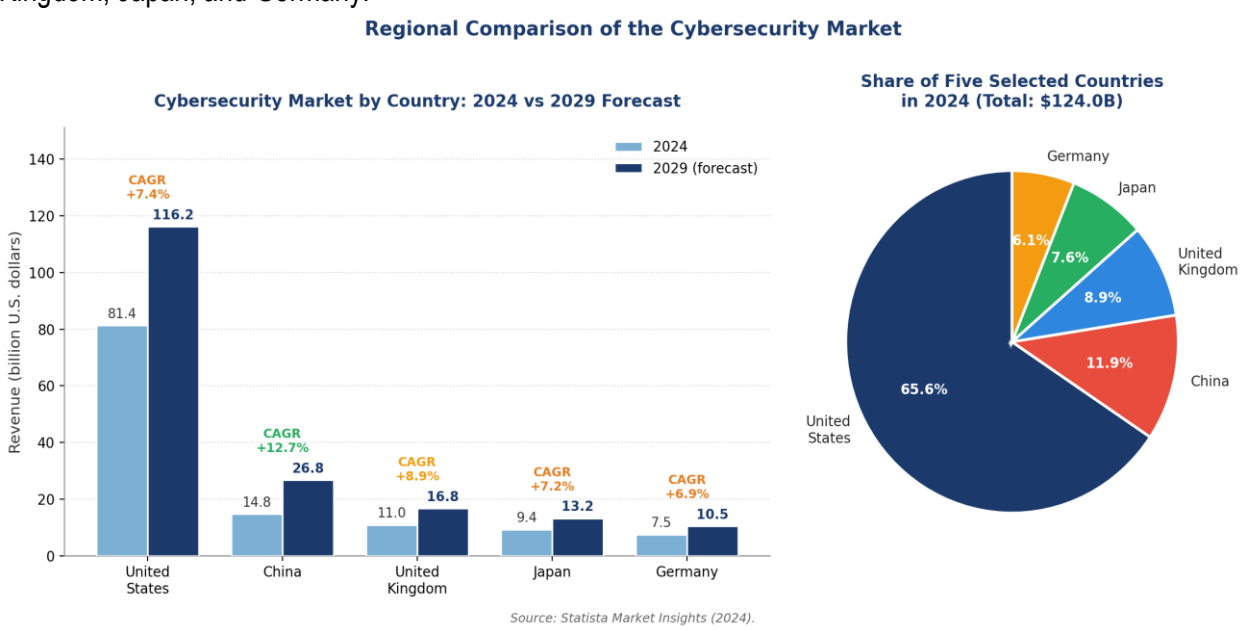


Figure 2 — Regional comparison of the cybersecurity market: size and forecast 2024 vs 2029
Source: constructed by the author based on data from Statista Market Insights (2024).

The analysis of the presented data allows us to make several key observations. First, the absolute market leader is the USA, with a volume of 81.37 billion US dollars in 2024, accounting for 65.6% of the total figure for the five countries (124.01 billion) and 43.8% of the global market (185.69 billion). According to the forecast, in 2029, the USA will maintain a dominant position with a volume of 116.20 billion US dollars. Such dominance is explained by several factors: the concentration of technology companies (Silicon Valley, Seattle, Boston, Austin), developed venture capital, aggressive state policy in national cybersecurity (Cybersecurity and Infrastructure Security Agency, CISA), and a high level of digitalization of the economy.

Secondly, China is showing the highest growth rate — a CAGR of 12.7% for the period 2024–2029 — which significantly exceeds those of other countries. The volume of the Chinese market will grow from 14.75 to 26.79 billion dollars. This is the result of a combination of the active state policy "Make China

DOI: 10.31379/sed.1.4.2025.38

Cyber Strong", large-scale investments in the development of national cybersecurity champions (Qi An Xin, NSFOCUS, Topsec, Hillstone Networks), and the growing awareness of the corporate sector about the need to protect its own infrastructure.

Thirdly, the markets of the UK, Japan, and Germany are showing stable growth at a CAGR of 6.9–8.9%. The UK remains the European leader in the industry due to its developed financial sector, high concentration of specialized personnel, and favorable regulatory environment. Japan is actively building cyber capabilities in response to growing threats from China and North Korea. Germany is a leader in continental Europe, especially in industrial cybersecurity (protection of OT/ICS environments in the manufacturing sector). More detailed calculations are provided in Table 2, our second calculation table 2.

Table 2 — Estimated indicators of the regional structure of the cybersecurity market, 2024 vs 2029

Country	2024 (billion dollars)	2029 (billion dollars)	Abs. growth	Rel. growth, %	CAGR, %	Share 2024, %
USA	81,37	116,20	34,83	42,80	7,40	65,62
China	14,75	26,79	12,04	81,63	12,70	11,89
UK	10,99	16,80	5,81	52,87	8,90	8,86
Japan	9,37	13,25	3,88	41,41	7,20	7,56
Germany	7,54	10,51	2,97	39,39	6,90	6,08
Top 5 Total	124,02	183,55	59,53	48,00	8,16	100,00

Source: calculated by the author based on data from Statista Market Insights (2024).

The data in Table 2 clearly demonstrate the extremely high level of market concentration. If we compare the relative shares of countries, the United States (65.62%) exceeds the sum of the other four countries (34.38%) by almost twice. Moreover, the volume of the American market alone (81.37 billion) exceeds the combined volume of the other four top-5 countries (42.65 billion) by 90.8%. In 2029, the situation changes somewhat in favor of the remaining countries (especially China), but the dominance of the United States remains at 63.30% of the five. The calculation of the Herfindahl-Hirschman Index (HHI) for the five countries yields a value of about 4,624 points, which is above the 2,500 threshold that the US Federal Trade Commission considers a sign of a "highly concentrated" market. If we calculate the indicator assuming the United States as the dominant player and the rest of the world as the only participant, the concentration will be even higher. This market structure has ambiguous consequences: on the one hand, it creates conditions for US innovation leadership and the global spread of American standards; on the other hand, it creates risks of unipolar dependence, especially for countries that strive for technological sovereignty (EU, China, India).

Special attention should be paid to the absence of India, Israel, South Korea, and Canada from the top 5 countries with powerful IT sectors. Israel is a particularly interesting case: despite the relatively small size of the national economy, this country occupies one of the leading places in the world export of cybersecurity technologies (companies Check Point, CyberArk, Imperva, Wiz, and others). This indicates that domestic demand for cybersecurity and the country's global role as a manufacturer of such technologies are distinct phenomena that do not always correlate linearly.

The sustained long-term growth of the global cybersecurity market is not a random phenomenon - it is due to the action of a complex of interrelated factors, which are useful to analyze in three groups: macroeconomic, technological, and behavioral.

According to Statista Market Insights (2024), global GDP for the period 2019–2029 will grow from 87.2 to a projected 138.3 trillion US dollars (CAGR of about 4.7%). This general economic upswing provides a strong basis for increased spending on cybersecurity. It is especially important that the share of spending on

DOI: 10.31379/sed.1.4.2025.38

cybersecurity in the structure of organizations' IT budgets is constantly growing - from approximately 6–8% in 2019 to 12–15% in 2024, according to various estimates.

A fundamentally important macro indicator is the level of Internet penetration. The global figure will increase from 52.3% in 2019 to a projected 86.5% in 2029. This means that by the end of the decade, almost 9 out of 10 people on the planet will have access to the Internet, and therefore potentially be in the zone of cyber threats. Every new billion Internet users is a new billion potential objects of attack (personal data, bank accounts, identifiers), and therefore a new billion potential consumers of cybersecurity products.

A separate category of macro factors is geopolitical events. The Russian-Ukrainian war, which has been ongoing since 2014 and entered a full-scale phase on February 24, 2022, has become a global catalyst for cybersecurity investment. Attacks by Russian state-run hacking groups (Sandworm, Fancy Bear, Cozy Bear) on Ukraine's energy, financial, telecommunications, and government infrastructure, as well as numerous attempts to target critical infrastructure in NATO countries and Ukraine's allies, have fundamentally changed perceptions of cyber threats in the business environment. According to industry experts, the war has led to an additional $15–25 billion in global cybersecurity spending during 2022–2024. In 2023–2024, this was compounded by the escalation in the Middle East and the increased activity of Chinese state-run hacking groups against Taiwan and ASEAN countries.

The second group of drivers concerns the transformation of corporate IT budget structures. According to the Flexera 2023 State of Tech Spend Report (based on a survey of 506 IT managers), in 2023, 66% of organizations planned to significantly increase cybersecurity spending, ranking it second in priority after AI/Machine Learning (68%). For comparison: in third place is Big Data/Analytics (60%), in fourth place is Automation (59%), then Cloud Operations (53%) and Cloud Migration (54%).

A special feature of this distribution is that cybersecurity is practically the only area not subject to cuts - only 5% of organizations plan to reduce it, while for Maintaining Legacy Systems, this figure reaches 27% (plan to reduce). This asymmetry indicates that corporate IT budgets are being actively reallocated from "obsolete" items (legacy system support) to "modernization" items (AI, cybersecurity, analytics, automation). Cybersecurity is one of the main beneficiaries of this reallocation.

Interestingly, the growth in cybersecurity spending is occurring in sync with that of AI/ML and cloud technologies. This is no coincidence: the implementation of AI and cloud infrastructure creates new vectors of cyber threats (data poisoning attacks on ML models, misconfigured cloud buckets, and secrets management in CI/CD pipelines), thereby generating additional demand for specialized cybersecurity solutions. Thus, the AI revolution not only does not compete with the cybersecurity market, but, on the contrary, it strengthens it.

The third group of factors is the direct increase in the intensity and sophistication of cyberattacks. The COVID-19 pandemic has caused a massive shift to remote work, significantly expanding the attack surface: home routers, employees' personal devices, and unprotected Wi-Fi networks have become potential points of entry for attackers. According to industry reports, the number of registered cyber incidents in 2020 increased by 30% compared to 2019, and the number of successful ransomware attacks by 150%.

Separately, it is worth noting the evolution of cybercrime's business model. If in the 2010s most attacks were carried out by relatively small hacker groups or individuals, in the 2020s an entire cybercrime "industry" with its own specialization has formed: developers of malicious software, operators of botnet infrastructure, sellers of stolen data on darknet markets, ransomware intermediaries (Ransomware-as-a-Service operators). Models such as "Cybercrime-as-a-Service" have become widespread, where non-specialized criminals can rent ready-made attack tools for a subscription fee. This has fundamentally lowered the threshold for entry into cybercrime and increased the total volume of attacks. The war in Ukraine in 2022–2026 has added new dimensions to this picture. First, it has legitimized the large-scale use of cyber operations as an instrument of state policy. Second, it led the authorities to downgrade some Russian cybercriminal groups from "tolerant" to "uncontrolled," thereby increasing the number of financially motivated attacks emanating from Russian cyberspace. Third, it deepened the gap between the "Western"

DOI: 10.31379/sed.1.4.2025.38

and “Eastern” segments of the global Internet, leading to a corresponding increase in the need to protect the digital infrastructure of both sides.

To understand how the cybersecurity market works, it is critical to analyze the specific structure of threats that organizations face and the cost of implementing them. Figure 5.1 presents a two-way analysis: the distribution of cyberattacks by type (according to NordVPN, March 2022 - March 2023) and the average cost of a data breach by industry (according to IBM Cost of a Data Breach Report 2023).

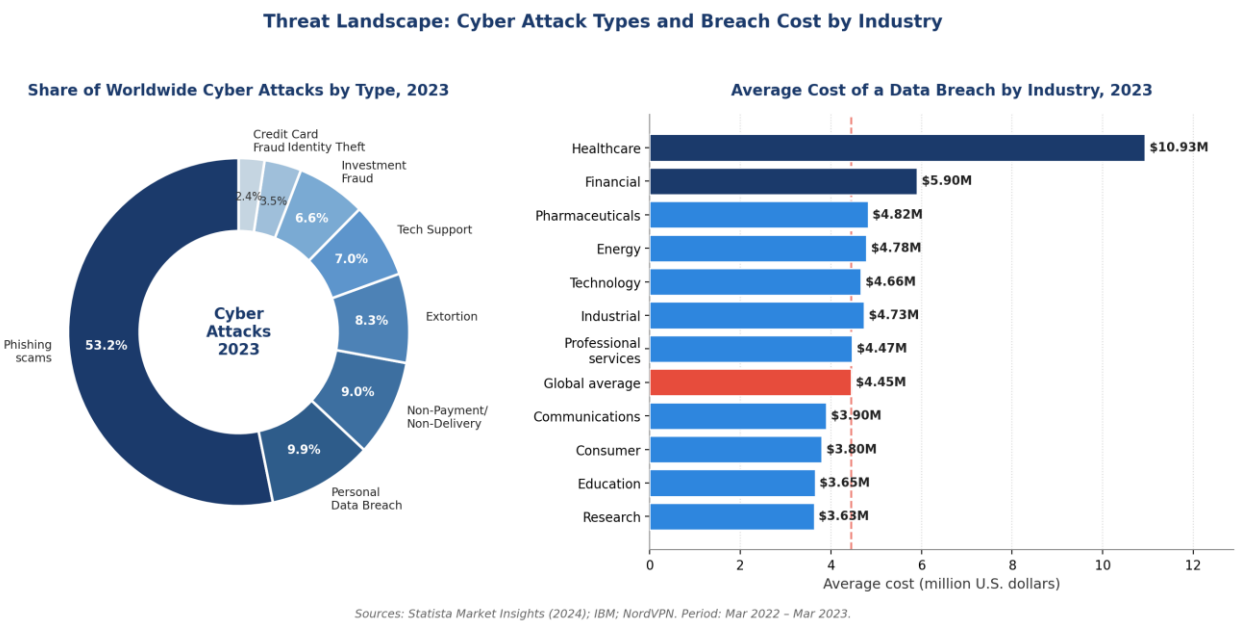


Figure 3 — Cyberthreat structure: distribution of attacks by type and average cost of data breach by industry, 2023. Source: constructed by the author based on data from Statista Market Insights (2024); IBM; NordVPN.

The left part of Figure 3 shows that phishing schemes remain the absolute leader among cyberattacks, 53.24% of all registered incidents. This indicator may seem unexpected to a non-professional observer — against the backdrop of active discussion of ransomware, APT campaigns, and artificial intelligence in cybercrime, it may seem that phishing is an outdated technique. However, the reality is the opposite: phishing remains the most effective attack vector precisely because of its simplicity, low cost, and focus on the weakest link in any security system — human psychology.

Modern phishing has evolved significantly. If in the 2000s it was rude letters from a “Nigerian prince”, then in the 2020s it is: 1) spear-phishing — targeted attacks against specific employees with prior intelligence; 2) BEC (Business Email Compromise) — imitation of letters from management with financial instructions; 3) AI-generated phishing campaigns using personalized texts and deepfake voice calls; 4) smishing — phishing via SMS; 5) vishing — phishing via voice calls. All of these options retain the basic principle: manipulation of human trust.

Second place is occupied by Personal Data Breach (9.94%) — violation of the integrity and confidentiality of personal data, often due to unprofessional actions of employees, incorrect system configuration, or successful hacking. Third place is Non-Payment/Non-Delivery (8.99%) — fraud in e-commerce. Next are Extortion (8.30%, mainly ransomware attacks), Tech Support Fraud (7.04%, fraudulent calls allegedly from technical support), and Investment Fraud (6.57%, especially relevant against the backdrop of the cryptocurrency boom and subsequent crash).

The right panel of Figure 3 shows the distribution of average data-leakage costs by industry. The undisputed leader is Healthcare — $10.93 million per incident, 2.46 times the global average ($4.45

DOI: 10.31379/sed.1.4.2025.38

million). Such extreme cost is explained by several factors: 1) high sensitivity of medical data, which means maximum fines from regulators (HIPAA in the US, GDPR in the EU); 2) high direct business costs — the need to notify patients, credit monitoring for victims, system restructuring; 3) potential lawsuits; 4) reputational losses, especially sensitive for medical institutions; 5) operational consequences — an attack can paralyze a hospital for weeks.

The second place is taken by the financial sector — $5.90 million per incident. The least “expensive” in terms of breach cost are the public sector ($2.60 million), hospitality ($3.36 million), media ($3.58 million), and retail ($2.96 million). It should be emphasized that the low “cost” does not mean that protecting these industries is less important — in many cases, it is simply a result of less stringent regulatory requirements and lower direct financial losses. The combined analysis of the threat and cost structure allows us to formulate several strategic conclusions. First, investments in phishing protection (anti-phishing solutions, staff training, MFA) remain critical due to the dominance of this attack vector. Second, regulated industries (medicine, finance, energy) require the highest level of cybersecurity investment due to the high costs of potential incidents. Third, the gap between industries in terms of leakage costs (from 2.60 to 10.93 million) indicates that unified “mid-market” cybersecurity spending benchmarks are of limited utility—each industry must be guided by its own ROI calculations.

The cybersecurity market is represented by a wide range of players — from specialized pure-players (Palo Alto Networks, CrowdStrike, Fortinet, Zscaler, SentinelOne, Check Point, CyberArk) to diversified technology conglomerates that include cybersecurity among their areas of activity. In this section, we will focus on the latter two — Microsoft Corporation and IBM, as they are the focus of the Statista Market Insights (2024) baseline report. Microsoft Corporation has emerged as one of the dominant global players in the cybersecurity market in the 2020s. The company’s combined annual revenue grew from $143 billion in fiscal year 2020 to $212 billion in 2023, representing a CAGR of 14% over the four-year period — twice the pace of the global cybersecurity market as a whole. Microsoft's revenue structure includes three key segments: Intelligent Cloud (Azure, server products, enterprise services) - $88 billion in 2023; Productivity and Business Processes (Microsoft 365, Dynamics, LinkedIn) - $69 billion; More Personal Computing (Windows, Surface, Xbox, advertising) - $55 billion.

Microsoft's strategic importance in the cybersecurity market is determined by several key assets. First, the dominant position of the Windows operating system in the corporate market, which makes Microsoft the main "host" of the business ecosystem and a natural supplier of security tools (Microsoft Defender, Windows Hello, BitLocker). Second, Azure's leading position as the second largest cloud platform in the world - Azure Sentinel, Azure Defender, Microsoft Entra ID are integrated solutions for cloud security. Third, the pervasiveness of Microsoft 365 as an enterprise collaboration ecosystem — Microsoft Purview, Microsoft Defender for Office 365 protect billions of enterprise users from phishing and other threats. Fourth, the world’s largest volume of cyber threat data (over 65 trillion signals per day), which offers unique opportunities to develop AI detection and response tools. According to Microsoft’s own estimates, the company’s cybersecurity revenue in 2023 exceeded $20 billion, making it one of the largest vendors in the global cybersecurity market. Microsoft’s intensive investments in security (over $4 billion per year in cybersecurity R&D), strategic acquisitions (CloudKnox, RiskIQ, Mandia, Aorato, Adallom), and integration of security features into core products form a holistic “secure by default” ecosystem.

IBM represents a different type of big player—a company with a long history that has undergone several transformations and is now focused on hybrid cloud solutions, AI, and cybersecurity. According to the IBM Annual Report 2023, the corporation’s annual revenue for the period 2020–2023 grew from $55 billion to $62 billion, corresponding to a CAGR of 3.9%—a much slower pace than Microsoft and moderate compared to the market average.

IBM’s revenue structure is divided between four main segments: Software — $26 billion in 2023 (up from $23 billion in 2020, +13%); Consulting — $20 billion (up from $16 billion, +25%); Infrastructure — $15 billion (down from $15 billion in 2020, which was the starting point of the down cycle); Financing — $1

DOI: 10.31379/sed.1.4.2025.38

billion (stable). The Other segment shrank to near zero, reflecting the completion of the divestment of non-core assets (the Kyndryl spin-off in 2021).

IBM occupies a unique niche in the cybersecurity market, focusing primarily on large corporations and government agencies. Key products include IBM Security QRadar (SIEM/SOAR platform), IBM Security Guardium (data protection), IBM Security Verify (identity management), and IBM X-Force Threat Intelligence (expert threat analytics). IBM's particular strength is its deep consulting expertise and ability to implement large-scale, comprehensive security transformation projects. The famous IBM Cost of a Data Breach Report, which we rely on in Chapter 5, is one of the most authoritative industry sources and an asset for promoting IBM's brand as an expert in cybersecurity.

Comparing Microsoft and IBM's strategies, we see they represent two distinct approaches to competing in the cybersecurity market. Microsoft is a large, integrated ecosystem where security is built into universal products; strategically, a pressing leader that leverages network effects and data scale. IBM is a highly skilled niche player that focuses on large customers with the highest security requirements; strategically, it is a deep expert that competes on quality and trust. Both strategies are viable, but they create different risk profiles: Microsoft grows faster but has a wider range of competitors; IBM grows slower but retains loyal customers with high margins.

Analysis of the structure and dynamics of the global cybersecurity market allows us to formulate several strategic prospects for its development by the end of the decade. The base scenario, which aligns with Statista Market Insights (2024) forecasts, assumes a volume of 271.90 billion US dollars by 2029, with a CAGR of 6.02% over the forecast period. Alternative scenarios may lead to both exceeding and failing to achieve these indicators.

Optimistic scenario: 320–360 billion US dollars by 2029

The optimistic scenario assumes market growth accelerates to a CAGR of 11–13% over the forecast period. The main driving forces of this scenario could be: 1) a serious aggravation of the geopolitical situation, which will force governments to sharply increase spending on national cybersecurity; 2) a series of large-scale cyber incidents that will dictate regulatory requirements for businesses (new laws such as the EU NIS2

irective, US SEC cybersecurity disclosure rules); 3) a breakthrough in quantum computing with the corresponding need for quantum-resistant cryptography; 4) the mass adoption of AI agents that require specific protection mechanisms.

Pessimistic scenario: $220–240 billion by 2029

The pessimistic scenario assumes a slowdown in growth rates to 3–5% CAGR. The main factors in such a scenario could be: 1) a global economic recession that will force corporations to reduce IT budgets; 2) market consolidation (M&A), when a smaller number of players will provide competitive pressure and price levels; 3) the emergence of radically new technological solutions (for example, AI-first security architectures) that will reduce the need for traditional products; 4) increasing geopolitical fragmentation of the market, which will reduce the potential of global players.

Discussion

In addition to uncertainty about growth rates, the cybersecurity market faces several systemic challenges. The first is an acute shortage of qualified personnel. According to the International Information System Security Certification Consortium (ISC²), the global shortage of cybersecurity specialists in 2024 was about 4 million people and continues to grow. This shortage limits the capabilities of both vendors (a lack of engineers for product development) and customers (a lack of specialists for implementation and operational support).

The second challenge is the rapid evolution of the threat landscape. The emergence of generative AI in 2022–2024 has created fundamentally new attack vectors: AI-generated phishing, deepfake deception,

DOI: 10.31379/sed.1.4.2025.38

poisoning of training data of AI models (data poisoning), and prompt injection attacks. Security systems must adapt to these new challenges faster than attackers can scale them — it's a constant race against time.

The third challenge is the growing complexity of IT environments. A modern corporation uses hundreds of SaaS applications, hybrid cloud architectures, employee mobile devices, IoT sensors, and OT systems. Each of these elements is a potential point of intrusion. Integrating security tools in such a fragmented environment becomes a separate engineering discipline (Security Mesh Architecture, Zero Trust models).

The fourth challenge is regulatory fragmentation. If in the 2010s the main regulatory frameworks were GDPR (EU, 2018) and HIPAA (US, medicine), then in the 2020s, NIS2 (EU, 2023), DORA (EU, 2024), SEC Cybersecurity Disclosure Rules (US, 2023), and numerous national laws (Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity", 2017) appeared. Global companies are forced to comply with dozens of incompatible regulatory regimes, creating a significant regulatory burden. Prospects for Ukraine: The cybersecurity market offers significant opportunities. First, the unique combat experience of protecting critical infrastructure from Russian aggression is a competitive advantage of Ukrainian specialists in the global expertise market. Secondly, European integration involves harmonizing cybersecurity requirements with EU norms (NIS2, DORA), thereby creating demand for consulting services and technological solutions. Thirdly, the post-war restoration of critical infrastructure should be carried out in accordance with the "secure by design" principle, thereby generating additional demand for modern cybersecurity solutions. Fourthly, Ukrainian technology companies have the potential to become exporters of cybersecurity solutions - especially in the niches of critical infrastructure protection, OT environments, and detection of state-owned APT groups.

Conclusions

The analysis allows us to formulate the following main conclusions.

The global cybersecurity market demonstrates sustainable long-term growth: from 89.72 billion US dollars in 2017 to a projected 271.90 billion in 2029. The total growth over thirteen years is 203.06%, or 3.03 times; the average annual growth rate (CAGR) is 9.68%. This is almost 2–2.5 times higher than the average growth rate of global GDP over the same period.

The market is divided into two main segments: Security Services ($97.30 billion in 2024, 52.4% of the volume) and Cyber Solutions ($88.39 billion, 47.6%). Structurally, the market is gradually shifting in favor of Cyber Solutions: in 2017, their share was 37.57%; in 2024, 47.60%; and in 2029 (forecast), 54.54%. This indicates the progressive automation of cyber defense through AI and machine learning.

The regional structure of the market is characterized by extremely high concentration: the USA, with a volume of 81.37 billion dollars in 2024, holds 65.6% of the combined market of five key countries and about 43.8% of the global market. China (CAGR 12.7%) demonstrates the highest growth rate, indicating the Chinese authorities' prioritization of national cyber capabilities. The United Kingdom, Japan, and Germany are growing at moderate rates of 6.9–8.9%.

The key drivers of the market are: (1) macroeconomic factors (growth in global GDP, Internet penetration from 52.3% in 2019 to 86.5% in 2029); (2) redistribution of corporate IT budgets in favor of cybersecurity (66% of organizations plan to increase); (3) increasing intensity and sophistication of cyberattacks due to the pandemic, the war in Ukraine, and the activation of state and financially motivated cybercriminal groups.

The structure of cyber threats is characterized by the absolute dominance of phishing schemes (53.24% of all attacks), which confirms the thesis about the human factor as the weakest link in security systems. The remaining 46.76% is distributed between Personal Data Breach (9.94%), Non-Payment/Non-Delivery (8.99%), Extortion (8.30%), and other types. The average cost of a data breach varies significantly by industry, from $2.60 million (government) to $10.93 million (healthcare), with a global average of $4.45

DOI: 10.31379/sed.1.4.2025.38

million.

The key corporate players in the market, Microsoft Corporation (CAGR 14% 2020–2023, annual revenue $212 billion) and IBM (CAGR 3.9%, revenue $62 billion), represent two fundamentally different strategies. Microsoft is a large-scale, integrated ecosystem focused on the mass market and ubiquitous use; IBM is a niche expert player focused on large corporate and government clients.

The scenario forecast for market development until 2029 provides for three possible trajectories: the base scenario ($271.90 billion, CAGR 6.02% in the forecast period), optimistic ($320–360 billion under conditions of accelerating geopolitical challenges and a breakthrough in quantum/AI), and pessimistic ($220–240 billion under conditions of global recession and technological consolidation).

Systemic challenges to the development of the industry are: an acute shortage of qualified personnel (about 4 million vacancies in the world as of 2024); rapid evolution of the threat landscape under the influence of generative AI; growing complexity of IT environments; and regulatory fragmentation of national legislation.

For Ukraine, the cybersecurity market opens up significant strategic opportunities: international recognition of expertise thanks to the experience of the Russian-Ukrainian cyberwar; integration into the European regulatory space; prioritization of the secure by design principle in the post-war restoration of critical infrastructure; export potential of domestic solutions in the niches of OT/ICS environment protection and APT analytics.

Prospects for further research. Promising areas of further research are: 1) a deeper analysis of the Ukrainian national cybersecurity market with the identification of niche segments of competitiveness; 2) quantitative modeling of the impact of geopolitical events on the dynamics of the global cybersecurity market; 3) research into the economics of cybercrime as a “mirror” segment of the cybersecurity market; 4) assessment of the impact of generative AI on both the supply of cybersecurity solutions and the evolution of cyber threats; 5) analysis of the effectiveness of corporate investments in cybersecurity through the prism of ROI and loss prevention.

References

1. Statista Market Insights. (2024). Cybersecurity Market Report. Hamburg: Statista. URL: https://www.statista.com/markets/424/topic/441/cyber-security/ [in English].
2. IBM Security. (2023). Cost of a Data Breach Report 2023. Cambridge, MA: IBM Corporation. URL: https://www.ibm.com/security/data-breach [in English].
3. Flexera. (2023). State of Tech Spend Report 2023: 506 IT Decision Makers Surveyed. Itasca, IL: Flexera Software LLC. [in English].
4. NordVPN. (2023). Global Cyber Attacks Report: March 2022 – March 2023. Vilnius: Nord Security. [in English].
5. Microsoft Corporation. (2023). Annual Report 2023 (10-K Filing). Redmond, WA: Microsoft Corporation. URL: https://www.microsoft.com/investor/ [in English].
6. International Business Machines Corporation. (2023). 2023 Annual Report. Armonk, NY: IBM. URL: https://www.ibm.com/investor/ [in English].
7. European Network and Information Security Agency (ENISA). (2024). Threat Landscape Report 2024. Athens: ENISA. [in English].
8. National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework 2.0. NIST CSWP 29. Gaithersburg, MD: NIST. [in English].
9. (ISC)². (2024). Cybersecurity Workforce Study 2024. Alexandria, VA: International Information System Security Certification Consortium. [in English].
10. European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333/80. [in English].
11. European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the

DOI: 10.31379/sed.1.4.2025.38

financial sector (DORA). Official Journal of the European Union, L 333/1. [in English].
12. U.S. Securities and Exchange Commission. (2023). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. SEC Final Rule 33-11216, July 26, 2023. [in English].
13. Verkhovna Rada of Ukraine. (2017). *Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" No. 2163-VIII (as amended 2024)*. URL: https://zakon.rada.gov.ua/laws/show/2163-19[in Ukrainian]
14. President of Ukraine. (2021). *Decree of the President of Ukraine "On the Cybersecurity Strategy of Ukraine" No. 447/2021*. Nagaichuk, N. H., Tretiak, N. M. https://zakon.rada.gov.ua/laws/show/447/2021[in Ukrainian]
15. Cybersecurity and Infrastructure Security Agency (CISA). (2024). Annual Performance Plan FY2024. Washington, DC: U.S. Department of Homeland Security. [in English].
16. Symantec / Broadcom. (2024). Internet Security Threat Report (ISTR) 2024. San Jose, CA: Broadcom Inc. [in English].
17. Verizon. (2024). 2024 Data Breach Investigations Report (DBIR). Basking Ridge, NJ: Verizon Communications Inc. [in English].
18. Gartner. (2024). Forecast: Information Security and Risk Management, Worldwide, 2022–2028. Stamford, CT: Gartner Research. [in English].
19. World Economic Forum. (2024). Global Cybersecurity Outlook 2024. Geneva: WEF. [in English].
20. Nagaichuk, N. H., Tretiak, N. M. Tkalenko, O. O. (2019). Strakhuvannia v systemi upravlinnia kiber-ryzykamy pidpryiemstva v umovakh tsyfrovoi ekonomiky [Insurance in cyber-risk management system of the enterprise in digital economy]. Finansovyi prostir – Financial space, 1, 97–116. Retrieved from http://nbuv.gov.ua/UJRN/Fin_pr_2019_1_8. [in Ukrainian]

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

Conceptualization: Lakhtionova Anastasiia
Data curation: Lakhtionova Anastasiia
Formal Analysis: Lakhtionova Anastasiia
Methodology: Lakhtionova Anastasiia
Software: Lakhtionova Anastasiia
Resources: Lakhtionova Anastasiia
Supervision: Lakhtionova Anastasiia
Validation: Lakhtionova Anastasiia
Investigation: Lakhtionova Anastasiia
Visualization: Lakhtionova Anastasiia
Project administration: Lakhtionova Anastasiia
Funding acquisition: –
Writing – review & editing: Lakhtionova Anastasiia
Writing – original draft: Lakhtionova Anastasiia

FUNDING

The authors received no funding for this article.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

DOI: 10.31379/sed.1.4.2025.38