SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2026
ORGANIZATION AND MANAGEMENT SERIES NO. 246

CYBERATTACKS ON BUSINESSES IN EU COUNTRIES – THE SCALE OF THE PHENOMENON AND ECONOMIC CONSEQUENCES

Monika ZIOŁO[1*], Krzysztof ZIOŁO[2]

[1] Department of Statistics and Social Policy, University of Agriculture in Krakow; monika.ziolo@urk.edu.pl, ORCID: 0000-0003-0884-4083
[2] SGH Warszawa; ziookrzysztof@gmail.com
* Correspondence author

Purpose: The aim of this article is to present the differences between EU countries in terms of the scale of cyberattacks on businesses in 2024 compared to 2022, considering various types of cybercrime. The dynamic development of technology and widespread digitisation has meant that companies in many countries are facing increasingly complex challenges in the area of cybersecurity. The consequences of cyber-attacks are multidimensional, including significant financial losses, serious operational disruptions such as downtime or data loss, and broad legal implications, including criminal liability of perpetrators but also civil liability of companies for data leaks.
Methodology: The scale of threats calculated as the change in the percentage of companies attacked by cybercriminals in 2024 compared to 2022. The data was obtained from the Eurostat database for the years 2022 and 2024. In a second step, EU countries were classified by the cyber-attacs on enterprises using a synthetic variable.
Findings: The synthetic variable effectively ranks countries in terms of risk levels, confirming the validity of the aggregation method used. The indicators analysed describe the percentage of companies experiencing specific forms of cyber-attacks (including phishing attacks, ransomware attacks, attacks on system availability and data breaches). Countries such as Denmark, Estonia and Latvia, with more developed cybersecurity policies, achieve better results in reducing the scale of cyber-attacks. In countries with lower synthetic variable values, such as Romania, Portugal and Bulgaria, it seems necessary to strengthen institutional support and intensify educational and investment activities in the area of corporate cybersecurity.
Practical implication: The countries exposed most at risk from cyber-attacks against businesses were identified. Countries where cyber threats have been significantly reduced were also presented. Countries with high synthetic variable values are characterised by significant percentage decreases in most of the analysed indicators, demonstrate high effectiveness of their cybersecurity strategies, and may serve as a benchmark for other countries in terms of protecting the digital infrastructure of enterprises.
Social implication: The article also highlights the costs incurred by companies, including social costs. These are related, among other things, to the disclosure of confidential data, loss of employment or financial resources.

Originality/value: The article deals with a very topical threat that is constantly growing. It lists the countries where companies are most vulnerable to cyberterrorist attacks. It also indicates the costs incurred by companies as a result of cyberattacks.
Keywords: cyber-attacks, financial consequences, operational consequences, legal consequences, hacking, cybercrime.
Category of the paper: research paper.

1. Cyber threats in today's business environment

The growing importance of cyberspace in society has brought about many changes on various levels. Companies have gained new distribution channels; public institutions have simplified numerous procedures for businesses and moved the application process online. We can shop, play the stock market, have psychotherapy sessions and even run a business on the internet. This new space has also opened up new opportunities for dishonest people. On the Internet, we encounter people who spread fake news, gain access to other people's data, and appropriate many goods belonging to others. Cybercrime is becoming more sophisticated every year, aided by the development of new mechanisms such as artificial intelligence and the refinement of old methods such as phishing.

People acting illegally or on the fringes of the law in cyberspace, who are one of the main threats to organizations, are recognized by the general public as hackers. Initially, the term 'hacker' did not have negative connotations, referring to people with high technical skills who pushed the boundaries of technology. As Majewski points out, hackers are a group of intelligent professionals specializing in a specific field, 'experts in programming and solving computer problems (Majewski, 2019). However, in common usage today, the term has an extremely pejorative meaning and is equated with "criminal" or 'computer burglar'.

The number of hackers is constantly growing, and research conducted in 2018 on a group of 169,827 respondents showed that over 90% of hackers are usually people under 35 years of age (over 90%), and 45.3% are between 18 and 24 years old. The main motivations for hackers include the desire to earn money (13.1% of respondents), the desire to learn (14.7%), meeting challenges (14%), fun (14%), the need to prove their skills (3%), career development (12.2%), helping others (8.5%), changing the world for the better (10%) and protection and defense (10.4%) (Fig. 1).

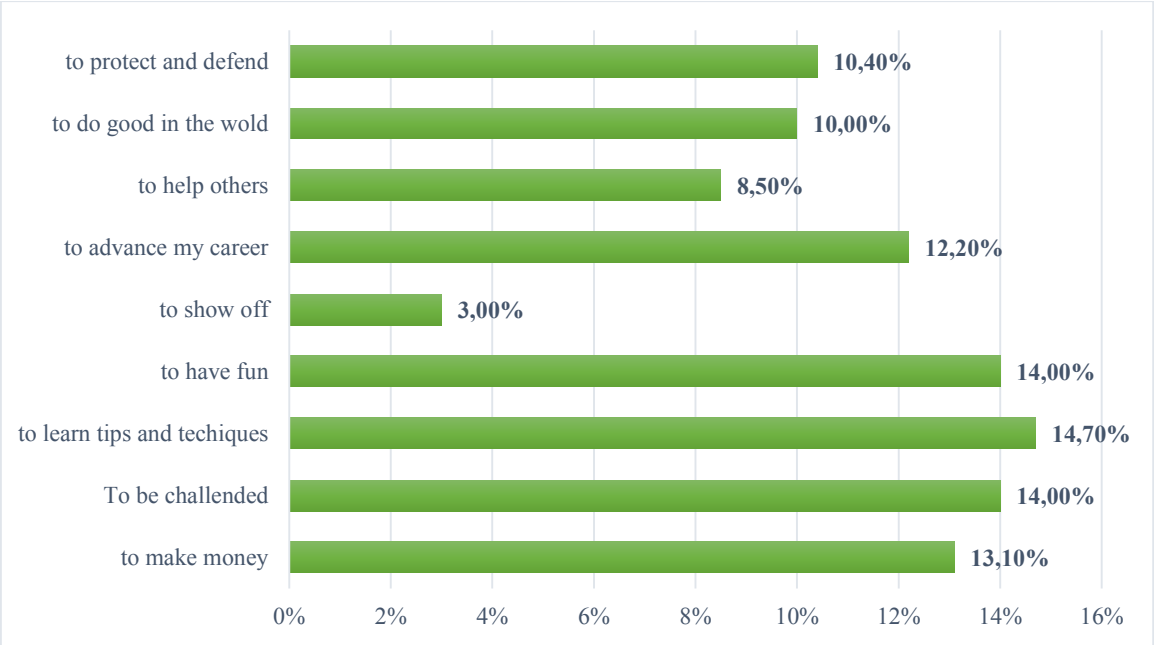

Figure 1. Hackers' main motivation.

Source: Hacker report, 2018, https://ma.hacker.one/rs/168-NAU-732/images/the-2018-hacker-report.pdf, 13.08.2025.

Hacker activities are harmful to both individual citizens and enterprises operating in all sectors of the economy. The purpose of the diagram (Fig. 2) is to present the main categories of threats in cyberspace, broken down into technical, organisational and human factors.

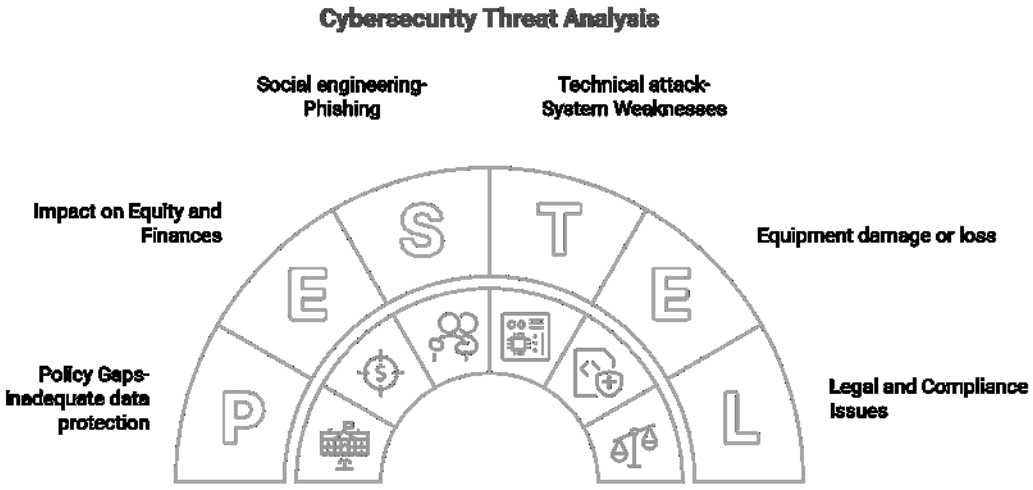

Figure 2. Cybersecurity threat analysis.

Source: Own study.

Among the most common difficulties caused by hackers are disruptions and downtime. Cyberattacks lead to significant disruptions and downtime in the daily operations of businesses. Another significant problem is data theft and sabotage (Fig. 2). Hackers can gain access to internal company information. This also applies to identity theft, installing spyware, sending viruses and destroying computer equipment. Examples include attacks on personal databases. Companies that store personal data of customers are vulnerable to attacks. There have been

cases where hackers have gained access to systems that are an integral part of equipment (e.g. for X-ray examinations) and devices containing personal databases of patients (e.g. for registration purposes). One way to attack a company's software is to infect its systems. Malware (viruses, worms, Trojans, backdoors, exploits, ransomware) can be spread by running an infected program, game, file, email attachment (including spam), and even through Trojan downloaders or botnets.

One of the most popular methods of attack is phishing and social engineering. Cybercriminals impersonate trusted institutions, companies, and even popular applications (e.g., WhatsApp) to steal data, passwords, or persuade users to install malicious software. These activities are often transferred to social media. Therefore, it is important to identify the scale of the phenomenon and monitor changes resulting from actions taken by companies.

2. Materials and Methods

The scale of cyber threats to businesses in EU countries was assessed based on annual data from 2022 and 2024. Four indicators were selected for analysis (Table 1).

Table 1.
Indicators describing the scale of cybercrime against businesses in EU countries

Variable	Full name
W_1	changes in the level of risk due to the loss or damage of confidential data [%]
W_2	changes in the level of risk due to phishing or pharming [%]
W_3	changes in the level of risk due to infection of malicious software [%]
W_4	changes in the level of risk due to ransomware attacks [%]

Source: Own study based on Eurostat. Available online: https://ec.europa.eu/Eurostat, 15 December 2025.

Their selection was preceded by a review of the literature, data availability, and statistical analysis (Table 2).

Table 2.
Basic numerical characteristics of indicators describing changes in cyber threats to businesses in EU countries in 2024 compared to 2022

Variable	min	max	mean	SD*	CV**	As
W_1	-26,27	42,51	-1,65	16,48	10,00	0,91
W_2	-53,93	78,13	13,51	37,68	2,79	-0,19
W_3	-53,54	91,67	-8,49	28,10	3,31	1,68
W_4	-29,74	79,47	-1,20	21,54	18,01	1,83

**CV – coefficient of variation, SD* – standard deviation.

Source: Own study based on table 1.

The greatest variation among the EU countries presented in the analysed period was in terms of the changes in the level of risk due to ransomware attacks indicator (Table 2). In 2024, compared to 2022, the coefficient of variation for this feature for EU countries was 180.1%. There are countries where companies have managed to reduce the threat posed by ransomware attacks in 2024 by as much as 30% compared to 2022. There are also countries where the scale of the threat posed by these attacks has increased by almost 90% over the two years analysed.

The most favourable changes in reducing cyber-attacks occurred in the case of infection of malicious software (W_3). In companies from the analysed countries, this represented an average decrease of 8.49%.

The largest increase in risk was caused by the W_2 indicator, changes in the level of risk due to phishing or pharming in the average increase was 13.51%.

The highest asymmetry coefficient was observed for indicator number 4 (1.83), which indicates that the list includes countries where companies observed an above-average increase in risks resulting from ransomware attacks.

In order to present the overall changes in the scale of the analysed threats in 2024 compared to 2022, directed against enterprises in EU countries, a synthetic index has been prepared.

This synthetic indicator for assessing the economic situation of enterprises in EU countries was prepared for each country in each year surveyed, it was determined according to the formula (Hellwig, 1968).

$$Q_i = \sum_{i=1}^{n} z_{ij} \tag{1}$$

where: Q_i - Synthetic indicator of cyber threat growth in EU countries in 2024 compared to 2022.

Due to the fact that the selected indicators are destimulants for determining the synthetic variable, the normalizing formula proposed in the MUZ method was used.

$$z_{ij} = \frac{\max x - x_i}{\max x - \min x} \tag{2}$$

Normalized value for *i* – indicator for *j* country.

The highest value indicates the best object in terms of the phenomenon under study.

The values of the synthetic measure allowed the objects under study to be divided into groups according to the following principle:

group I (very high level): $Q_i \in \left(\overline{Q} + S_Q; \max_i Q_i\right]$,

group II (high level): $Q_i \in \left(\overline{Q}; \overline{Q} + S_Q\right]$,

group III (medium level): $Q_i \in \left(\overline{Q} - S_Q; \overline{Q}\right]$,

group IV (low level): $Q_i \in \left[\min_i Q_i; \overline{Q} - S_Q\right]$,

where $\overline{d}$, S_d - the arithmetic mean and standard deviation of the values, respectively

Q_i defined according to the formula (1).

3. Results

Indicators: $W_1; W_2; W_3; W_4$ are destymulants, hence the rankings of countries by indicator values in 2024 compared to 2022 are presented in descending order in figure 1. High indicator values indicate that countries in 2024, compared to 2022, have reduced the scale of threats caused by cybercrime.

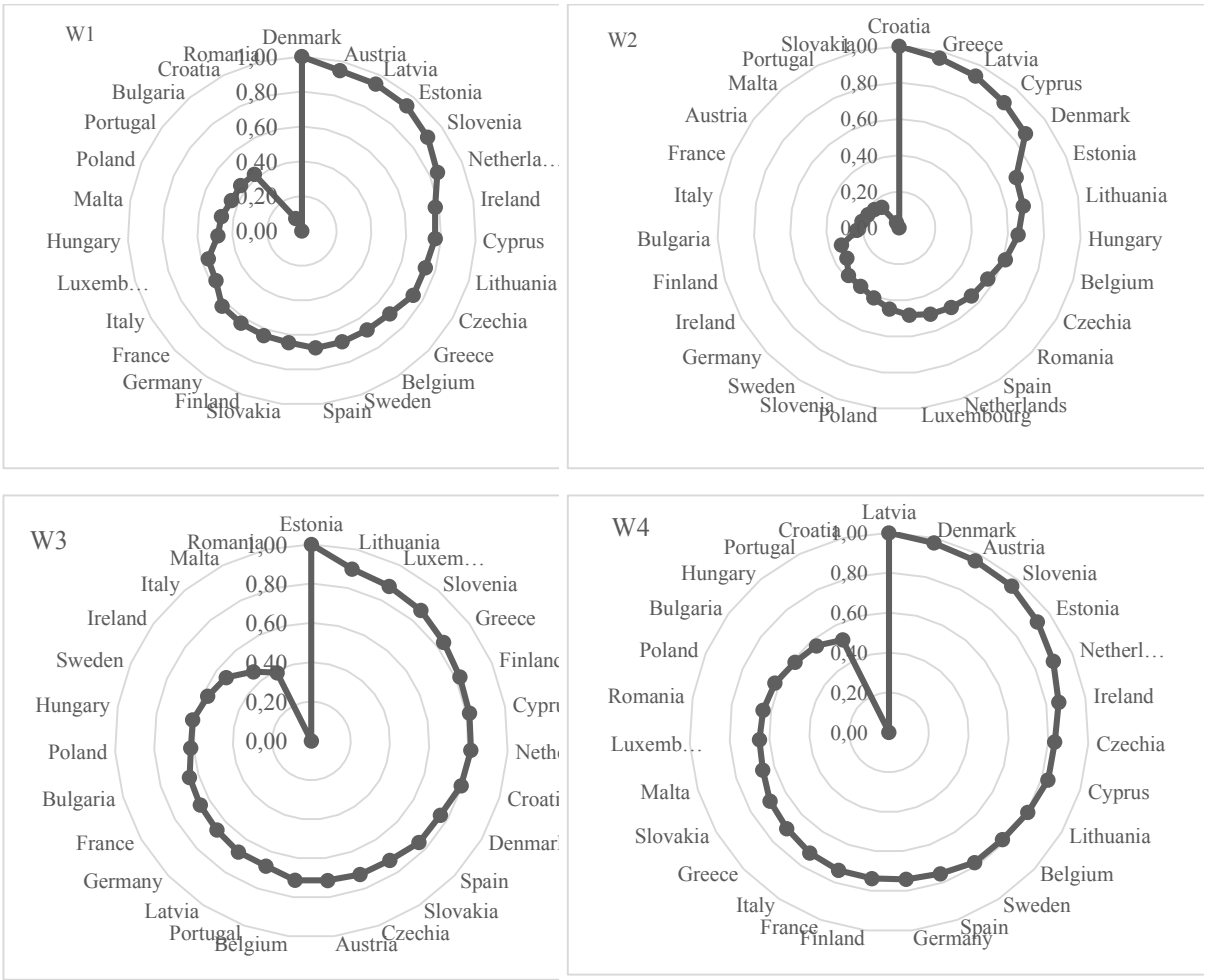

Figure 2. Rankings of EU countries according to standardized indicator values in 2024 compared to 2022.

Source: Own study based on designations as in Table 1.

The first indicator (W_1) describes ICT security incidents leading to: ICT service unavailability, data destruction or damage, and disclosure of confidential data. Changes in this indicator are most unfavorable in Romania, Croatia and Bulgaria (Fig. 2). The scale of this threat in 2024 compared to 2022 increased for companies operating in these countries by 42.51%, 37.01% and 13.31%, respectively. Eighteen countries have managed to reduce the scale of such cyberattacks. The most favourable changes were seen in Denmark (-26.27%), Latvia (-22.43%) and Austria (-22.58%).

The threat posed by pharming, phishing attacks (W_2), and actions by own employees (intentionally or unintentionally) increased in 18 countries. The largest increases were in Slovakia (78.13%), Portugal (73.85%) and Malta (58.50%). The most significant improvements in reducing phishing and pharming attacks were seen in Croatia, where the number of attacks on businesses fell by more than half (53.93%), as well as in Greece (48.72%) and Latvia (45.52%).

Threats due to infection by malicious software or unauthorized intrusion, hardware or software failures (W_3) in 2024 compared to 2022 have been reduced in companies in 20 countries. The scale of this phenomenon has been significantly reduced in Estonia (by 53.54%), Lithuania (38.81%) and Luxembourg (36.13%). Cybercrime has increased significantly in Romania (91.67%), Malta (35.27%) and Italy (25%).

In 16 countries, the scale of threats related to ransomware attacks, hardware or software failures increased (W_4). The largest increase in the number of threatened companies was in Croatia (79.47%), Hungary (17.13%) and Portugal (22.89%). In Denmark, Latvia and Austria, on the other hand, the scale of threats affecting companies decreased by 27%, 29.74% and 25.62%, respectively.

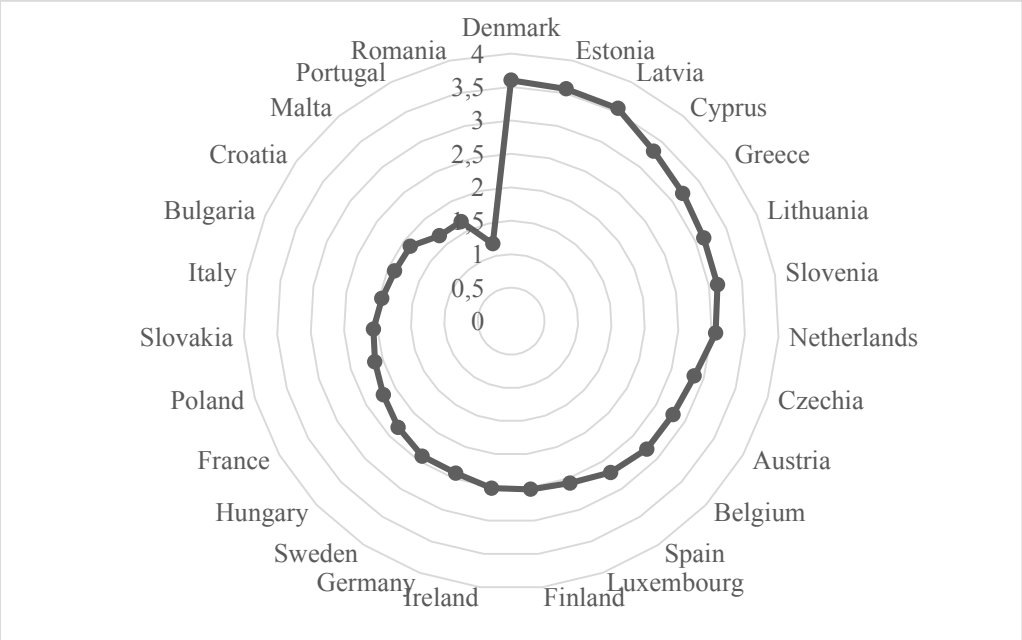

Figure 3. Rankings of EU countries by indicator value Q_i in 2024 compared to 2022.

Source: Own study based on Eurostat.

Countries such as Denmark, Estonia and Latvia are characterised by relatively high synthetic variable values. This means that companies in these countries have effectively reduced the scale of cyber-attacks in 2024 compared to 2022 (Fig. 3). These countries can be considered leaders in improving cybersecurity, which may be due to advanced protection systems, a high level of threat awareness and stable institutional frameworks.

In contrast, Romania, Portugal, Croatia and Bulgaria achieve relatively low synthetic variable values. This indicates the limited effectiveness of measures taken by companies to reduce cyber threats. In these countries, the level of risk has remained high or has only decreased slightly, and in some cases has even increased.

Cyberattacks cause many adverse situations for businesses. Therefore, the costs and losses associated with hacker activity can be divided according to various criteria. Below are some of them that are often cited in the literature on the subject.

4. The financial consequences of cyber-attacks for businesses

In the literature on the subject, the costs associated with cybersecurity and the consequences of data breaches are classified according to several complementary models that allow organizations to analyses risks and plan expenditure more accurately.

The most common division is into three main categories:

- Direct costs: These include measurable expenses incurred to ensure protection and repair damage after an attack. They include the purchase and maintenance of protective technologies (antivirus software, firewalls, intrusion detection systems), legal fees, the cost of recovering lost data, and expenditure on audits and certification of compliance with standards (Wygodny, 2021). In the event of a data breach, this group also includes the costs of protecting the identity of affected consumers and financial compensation (Dymek, 2024).
- Indirect costs: These relate to preventive and operational activities that are not the result of a specific incident but are necessary for the functioning of the security system (Korszewski, Oreziak, Wielec, 2021). These include employee training, cyber insurance premiums, specialist consulting and the remuneration of personnel responsible for cyber security (Pelc, 2021).
- Hidden (or opportunity) costs: These are the most difficult to estimate, but can have the most devastating impact on a company in the long term (Fuksiewicz, 2023). They include loss of reputation and customer trust, disruption to operations, lost contract revenue, brand devaluation, and loss of intellectual property. Nakashima and Robertson, referring to Sony's PlayStation data breach in April 2011, commented that the costs can be significant in terms of damage to a company's reputation (Nakashima, Robertson, 2011). Ash Raghvan (Deloitt, 2016) points out the non-obvious and long-term effects of attacks, which are difficult to estimate. Liu and Kuhn, on the other hand, argue that: ‘Depending on the type of data loss that has occurred, an organization may experience different types of consequences, but in almost all cases these include both financial costs and reputational costs’ (Liu, Kuhn, 2010).

Deloitte, on the other hand, divides the costs resulting from a cyberattack into 'above-the-surface' (better known as the costs of cyber incidents) and 'below the surface' costs (hidden or less visible costs) — a total of 14 categories (Deloitte, 2016), as presented in Table 2. Classification according to the 'Iceberg' model (Deloitte). The literature also cites a model that divides costs into those that are visible 'above the surface' and those that are hidden 'below the surface'.

- Above-surface costs: Well-known expenses such as technical investigations, notifying customers of the breach, and public relations costs.
- Below-the-surface costs: Long-term effects, including increased external financing costs, loss of customer relationships, and loss of competitive advantage.

Table 1.
Sharing of costs incurred by businesses in connection with cyber attacks

Above-surface costs	**Below-the-surface costs**
Conducting a technical investigation	increase in insurance premiums
Notifying customers of the breach	increase in debt costs
Protecting customers after the breach	effects of reduced operational activity or destruction
Compliance with regulatory requirements	lost value of customer relationships
Public relations costs	value of lost revenue
Legal advisory fees and court costs	devaluation of the company's reputation
Improving cybersecurity	loss of intellectual value

Source: Study based on Krawczyk-Jezierska, 2016.

The structure of these costs can be compared to an iceberg: expenditure on software or legal assistance is only the tip of the iceberg visible above the water, while beneath the surface lie much more powerful and difficult to measure losses, such as damaged reputation or loss of market advantage, which can ultimately lead to the sinking of the entire organization.

The International Monetary Fund (IMF) and consulting firms propose dividing costs according to the stage of the organization's activities, distinguishing between costs before and after a cyberattack. This division further distinguishes between the preventive phase and the associated cybersecurity costs:

1. Preventive phase: Costs of ongoing system maintenance and compliance with legal requirements.
2. Reactive (immediate) phase: Expenses for stopping the attack, technical investigation and informing victims.
3. Impact Management: Short-term costs of data recovery and handling legal claims.
4. Business recovery and repair: Long-term investments in new processes and systems and dealing with lower demand for the company's services after the incident. The financial losses resulting from cyber-attacks are enormous and are growing steadily.

In order to prevent cyber-attacks, companies should take a number of measures, including the following.

5. Preventing and managing the risk of cyber-attacks in businesses

Effective prevention of cyber-attacks requires a comprehensive approach, including both preventive and intervention measures. It is necessary to educate people about social values and skills, as well as how to use digital technology, recognize threats and prevent them. Such training should be mandatory. For companies, this also means raising employee awareness about phishing and other social engineering attacks.

In terms of technological security, it is important to install antivirus software and a firewall, and to regularly check the status of antivirus software installations and updates on all devices connected to the network. The operating system, web browsers and other programs should be updated regularly.

Employees and users should use strong and unique passwords. You should set complex passwords yourself, change them regularly and not use the same password for multiple accounts.

Employees should not open suspicious emails, click on links, open attachments from unknown senders, install software from unknown sources, or visit websites with illegal content. It is important to make regular backups of company files.

Employees should also minimize use of open Wi-Fi networks and, when using them, do not share sensitive data or logos.

6. Conclusion

In the face of rapid technological development and widespread digitalization, businesses in countries are facing increasingly complex challenges in the area of cybersecurity. The consequences of cyberattacks are multidimensional, including significant financial losses (amounting to trillions of dollars globally), serious operational disruptions (downtime, data loss) and broad legal implications (criminal liability of perpetrators, civil liability of companies for data leaks).

Available sources emphasize that despite the growing threat, many companies still do not treat cybersecurity as a priority, allocating negligible resources from their IT budgets and lacking adequate response procedures. Low awareness among users (both company employees and the general public) of basic threats such as phishing and malware further facilitates the activities of cybercriminals.

Negative percentage changes indicate a decrease in the percentage of companies affected by cyber-attacks, which should be interpreted as a positive effect of protective measures. Positive values indicate an increase in the scale of attacks and, consequently, a deterioration in

the cybersecurity situation. Significant percentage decreases are observed in many countries, which may indicate the implementation of more advanced protection systems, increased employee awareness, and more effective implementation of EU regulations (e.g. the NIS Directive).

The synthetic variable was constructed as an aggregate of standarised percentage changes in partial indicators (W1-W4). The higher the value of the synthetic variable, the greater the degree to which cyber-attacks have been mitigated by enterprises in a given country. In methodological terms, it serves as a synthetic measure of the effectiveness of companies' preventive and adaptive measures against cyber threats.

Countries with high synthetic variable values are characterised by significant percentage decreases in most of the analysed indicators, demonstrate high effectiveness of their cybersecurity strategies, and may serve as a benchmark for other countries in terms of protecting the digital infrastructure of enterprises.

The results confirm that the level of cyber threats is not uniform across Europe. Countries with a higher level of digital development, such as Denmark, Estonia and Latvia, with more developed cybersecurity policies, achieve better results in reducing the scale of cyber-attacks. At the same time, high exposure to digital technologies means that even in these countries, threats remain a significant challenge. In countries with lower synthetic variable values, such as Romania, Portugal and Bulgaria, it seems necessary to strengthen institutional support and intensify educational and investment activities in the area of corporate cybersecurity.

Effective defense against cyberattacks requires a comprehensive strategy that combines education at all levels (from the youngest users to company management), the implementation of advanced technological security measures, and the development of clear incident response procedures. It is also necessary to increase cooperation between companies, law enforcement agencies and service providers in order to build a more resilient digital environment and minimize the negative effects of cybercrime. Without these measures, the operational, financial and legal risks for businesses will continue to grow.

References

1. Deloitte (2016). Beneath the surface of a cyberattack. A deeper look at business impacts.
2. Dymek, J. (2024). *Badanie poziomu realizacji założeń cyberbezpieczeństwa firm i instytucji Unii Europejskiej*. Wrocław: Wydawnictwo Uniwersytetu Ekonomicznego, p. 119, https://dbc.wroc.pl/Content/130415/Dymek_Badanie_poziomu_realizacji_zalozen_cyberbezpieczenstwa.pdf, 07.12.2025.
3. *Eurostat - EU SMEs: An Overview* (2024). European Commission.

4. Fuksiewicz, M. (2023). Rodzaje i natura cyberataków oraz zarys działań w obszarze cyberbezpieczeństwa infrastruktury informatycznej. *Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu,* p. 57, https://doi.org/10.58683/dnswsb.615, 08.12.2025.
5. Hacker report (2018). https://ma.hacker.one/rs/168-NAU-732/images/the-2018-hacker-report.pdf, 13.08.2025.
6. Hellwig, Z. (1968). Zastosowanie metody taksonomicznej do typologicznego podziału krajów ze względu na poziom ich rozwoju oraz zasoby i strukturę wykwalifikowanych kadr. *Przegląd Statystyczny, Vol. 4,* pp. 307-327.
7. Hellwig, Z. (1974). A Method for the Selection of a „Compact" Set of Variables. In: *Social indicators: problems of definition and of selection, Methods and Analysis Division, Reports and papers in the social sciences, no. 30.* UNESCO, Department of Social Sciences.
8. Koszewski, R., Oręziak, B., Wielec, M. (2021). *Wdrożenie metod i instrumentów zapobiegania przestępczości w organizacjach.* Warszawa: Wydawnictwo Instytutu Wymiaru Sprawiedliwości, p. 88.
9. Krawczyk-Jezierska, A. (2019). Koszty instytucji finansowych w świetle zagrożeń cybernetycznych (Costs of financial institutions in the light of cyber threats). *Przegląd ustawodawstwa gospodarczego, vol. LXXII, no. 8(854)*, doi: 10.33226/0137-5490.2019.8.4
10. Liu, S., Kuhn, R. (2010). Data Loss Prevention. *IT Professional, 12,* 10-13.
11. Majewska, K. (2019). The electronic register in Polish schools: Studies from the level of early school education. In: D. Siemieniecka (ed.), *Virtuality and education: Future prospects* (pp. 93-111). Toruń: Adam Marszałek.
12. Nakashima, R., Robertson, J. (2011). *Credit data risked in PlayStation outage*. https://www.eschoolnews.com/2011/04/27/sony-credit-data-risked-in-playstation-outage/, 15.12.2025.
13. Pelc, P. (2021). Wybrane regulacje dotyczące cyberbezpieczeństwa instytucji finansowych. *Cybersecurity and Law*, p. 135, https://bibliotekanauki.pl/articles/1987417.pdf, 08.12.2025.
14. Wygodny, A. (2021). *Metody prowadzenia audytu cyberbezpieczeństwa - ustawa o KSC*. Najwyższa Izba Kontroli, pp. 85-86, https://www.nik.gov.pl/plik/id,23959.pdf, 15.02.2025.