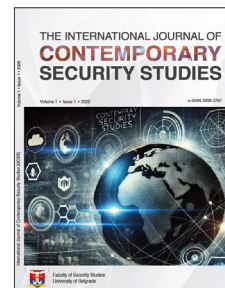


Faculty of Security Studies, University of Belgrade  
**International Journal of Contemporary  
Security Studies (IJCSS)**



## Economic Aspects of Cyber Security: Socio-Financial Consequences of Cyber Attacks

Nikola Vidović\*, Hatidža Beriša<sup>2</sup>

1 University of Belgrade, Faculty of Security Studies, Gospodara Vučića 50, 11050 Belgrade, vidovicnikola.finance@gmail.com.

2 University of Defence, Military Academy, Belgrade – Republic of Serbia, Veljka Lukića Kurjaka 1, 11000 Belgrade, hatidza.berisa@mod.gov.rs.

\* Correspondence: hatidza.berisa@mod.gov.rs

Received: 3 March 2025; Revised: 17 April 2025; Accepted: 2 June 2025; Published: 30 June 2025

### ABSTRACT

Conceptualising the economic aspects of cybersecurity, this research's analytical framework reveals the cause-and-effect relationship between risk and threat in cyberspace, as well as the materialisation of damage outside the digital framework. It includes vulnerability and exposure factors, as well as security measures that influence the observed phenomenon and cyberspace. A systematic analysis of the costs caused by the same financial damage, as well as the economic and social consequences that arose from them, was carried out on a relevant sample of cyber attacks in the time interval from 2009 to 2024 and concerns natural and legal persons, state administration bodies and individual countries of the world, international companies, large, medium and small enterprises, financial institutions and critical infrastructure. Proactive cybersecurity measures, effective incident response planning, cyber insurance, and integration of cyber risk into corporate governance are crucial to mitigating the impact of cyber attacks on all business entities, both in the public and private sectors of the economy, at the national, international, and global levels.

### KEYWORDS

Cybersecurity, cyber attacks, economy, consequences, finance.

## 1. Introduction

Cybersecurity has become a key aspect of global economic development, as well as of every national economy, which is reflected in the integrity of economic systems and financial flows, as well as their dependence on digital platforms. The world today faces a polarised geopolitical order, multiple armed conflicts, scepticism regarding the implications of future technologies, global economic uncertainty, and the emergence of a digitalised social community (Lis & Mendel, 2019; Zadorozhnyi et al., 2021; Ryan & Soderber, 2024; Thakur, 2024). Amid this complex landscape, according to the World Economic Forum (2024), the cybersecurity economy has grown exponentially faster than the overall global economy and outpaced growth in the technology sector, with varying impacts on high-income and developing countries, as well as businesses and governments, due to the contours of the cyber threat landscape (Kuzior et al., 2024), macroeconomic trends, regulations, and the time required to adopt technologies. The rising cost of access to innovative cyber services, tools, skills, and expertise continues to impact the global economic system's ability to build safer cyberspace, particularly amid numerous transitions, where more than 60% of all financial transactions are conducted online (Valackienė & Odejai,

2024). Innovations created by the globalisation process, the digital transformation of the economy (Slavković et al., 2023), and the establishment of sustainable growth and development of technological achievements are integrated into the structures of many countries due to their capacity to generate double value for both customers and business organisations.

They are also key drivers of intensive economic growth and determinants of the effects that accumulate in economic activities. Given that the evolution of new technologies is based on artificial intelligence (AI), blockchain databases (Saeed et al., 2023), and quantum and cloud computing (Cloud), we are faced with the security of data transmission, which is a key asset in the digital age (Weng & Wu, 2024) and the challenges of cybersecurity, which is precisely the consumer society as a sociological category, with its consumerisation, putting it in the focus of new research (International Telecommunication Union, 2024). The expansion of user functions provided by digitalisation has encouraged the development of products and services in the virtual space, emphasises Tarter (2017), which has caused a dynamic change in the operating environment, where the information society has acquired a dominant and growing dependence on information and communication technologies (ICT) referred to by the authors (Bederna & Szádeczky, 2023), but also exposure to a growing range of negative impacts (Fotis, 2024) directly on all those who work in the same business and private life, and indirectly on those who depend on them in the physical world (Issayeva et al., 2023).

Cybersecurity threats and incidents in cyberspace negatively impact the market value of business entities, revenue, profit, reputation, brand, market capitalisation, intangible assets, and financial policies of companies (Issayeva et al., 2023). For this reason, the paper comprehensively analyses the impact of cyber attacks and incidents on company performance, investments and financial policies, relying on the methodology used in previous empirical research. Publicly disclosed cyber incidents are growing globally, with an annual growth rate of 21%. This acceleration is most pronounced in Latin America and the Caribbean, as well as in countries with higher middle incomes (Cobos, 2024).

## **2. Financial factors and implications for cyber security**

The digitalisation of social activities has led humanity to rely heavily on the reliability, security, and integrity it provides, thanks to the efficiency of computer automation in performing everyday tasks. Every social phenomenon is accompanied by various aspects and outcomes that arise from it - and, looking at it generally, these can be both positive and negative effects. The expansion of user functions provided by digitalisation has encouraged the development of products and services in the virtual space but also exposure to a growing range of negative impacts directly on all those who work in the same business and private life and indirectly on those who depend on it in the physical world (Tarter, 2017).

Several complex factors are leading to the escalation of the complexity of the cyber landscape, primarily geopolitical tensions that contribute to a more insecure environment, then increased integration and dependence on more complex supply chains lead to a more unclear and unpredictable risk landscape (Onunka et al., 2023; Vidović et al., 2024), while the rapid adoption of new technologies and new technologies contribute to new threats. Meanwhile, the increasing number of international regulatory requirements adds a compliance burden for organisations. All of these challenges are exacerbated by a growing skills gap, which further complicates the ability to effectively manage cyber risks (World Economic Forum, 2025).

**Table 1.** Overview of key requirements for reporting cyber incidents and attacks in the US, EU, UK, Japan, Singapore and South Korea

State/Region	Agency	The Basics of Cyber Incident and Attack Reporting	Type of report	Time frame
USA	CISA	CIR CIA	Entities report and report all covered cyber incidents to the Agency (CISA)	72 hours
		Federal Initiative for the Sharing of Incident Reports	Any federal entity that receives a report of a cyber incident must share that report with the CISA	24 hours
		CIR CIA - Ransomware payments	Reporting all ransom payments made as a result of ransomware attacks	24 hours
	SEC	Cyber Security Risk Management, Strategy, Management, and Incident Detection	Disclosure of Cyber Security and Information Incidents by Public Companies	4 days
	NCUA	Cyber Incident Notification Requirements	Notification to all federally insured credit unions of a cyber incident reported by affiliates	72 hours
	US-CERT	Federal Law on the Modernization of Information Security	Federal Agency Report on Incidents Where Confidentiality, Integrity, and Availability Are Compromised	1 hour
EU	ANISA	EECC	Report on cyber incidents affecting the confidentiality, authenticity, integrity and availability of assets	Without delay
		EU Cyber Resilience Act	Preliminary notification of the incident to the relevant national authority	24 hours
	CSIRTs	Regulation on Network and Information Systems (NIS 2 European Commission Directive No. 2022/2555)	Initial Notice, Intermediate Report and Final Report	24 hours 72 hours 1 month
	National Supervisory Authority	DORA	Report on Significant Incidents in ICT Systems by Financial Institutions	24 hours
	National Supervisory Authority	GDPR	Report on the violation of personal data of the organisation	72 hours
UK	NCSC	NIS Directive 2018	Cyber incident report and notification to competent authorities from operators of essential services and digital service providers	72 hours
		Cyber Security and Resilience Act	A comprehensive report on cyber attacks and incidents against state authorities	Indefinite
	National Supervisory Authority	UK General Data Protection Regulation (GDPR)	Notification of theft of personal data as a result of a cyber attack	72 hours
Japan	PPC	APPI	Reporting on the violation and theft of personal data of all organisations and entities operating	3-5 days
		Fundamental Law on Cyber Security	Cyber Attack Notification	3-5 days
	FSA	Financial Services Agency (FSA) Guidelines for the Protection of Personal Data in the Financial Sector	Report of all entities in the financial sector on the theft of data and funds	Right away
	Ministry of the Interior and Communications	Law on Business in the Field of Telecommunications	Reporting of incidents that lead to the interruption of ICT services and affect the personal data of ICT users	No further ado
	NISC	Common Standards on Information Security Measures of State Entities	Instant report of a cyber incident and attack	Right away
Singapore	CSA	Cyber Security Law	Critical Infrastructure Operator's Reporting of Significant Incidents and Attacks	2 hours
	Commission for Personal Data Protection	The Personal Data Protection Act (PDPA)	Notification of a significant cyberattack that causes massive damage and affects 500 or more individuals in the service	72 hours
South Korea	PIPC	The Personal Information Protection Act (PIPA) and the Law on the Use and Protection of Credit Information	Three notifications depending on the damage caused to the data (lost, stolen, discovered)	1-5 days

Source: Authors based on data from Petit (2024).

Narrowing the focus to the business context, two concepts closely related to harm are “*impact*” and “*risk*”. Both of these concepts are pervasive in economic empirical research, literature, and practice, as Agriofotis et al. (2018) point out, as they represent the activity of one or more individuals, which can lead to a positive or negative outcome through cause-and-effect relationships. This characterisation of impact as a generic term is supported by others in the security field across academia and government, as well as numerous agencies responsible for digital security, such as the European Union Agency for Network and Information Security (ENISA), which defines impact as the result of an unintended incident, and which is embedded in the understanding of the principles established by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). Some describe the impact as the potential harm that can be expected to result from unauthorised actions or loss of confidentiality, integrity, or availability, and it is these manifestations that have received special attention in this research. The analysis is therefore focused primarily on harm, with the intention of emphasising the impact of a cyberattack as undesirable. Although impact is a non-specific term, in security, it often implies a negative outcome. Many companies vastly underestimate the costs of security breaches (Cashell et al., 2004); for these reasons, a reporting system has been established from leading global, international and national organisations and agencies, shown in Table 1, which monitor, control and establish a proper cost measurement system, which suggests to decision-makers in business entities the level of investment expenditures on improving the cybersecurity of the business environment in cyberspace.

### 3. Accounting treatment of cyber attack costs

When analysing the costs of cyberattacks, the IBM Corporation (2024) identified patterns in business activities that tend to either reduce or increase them.

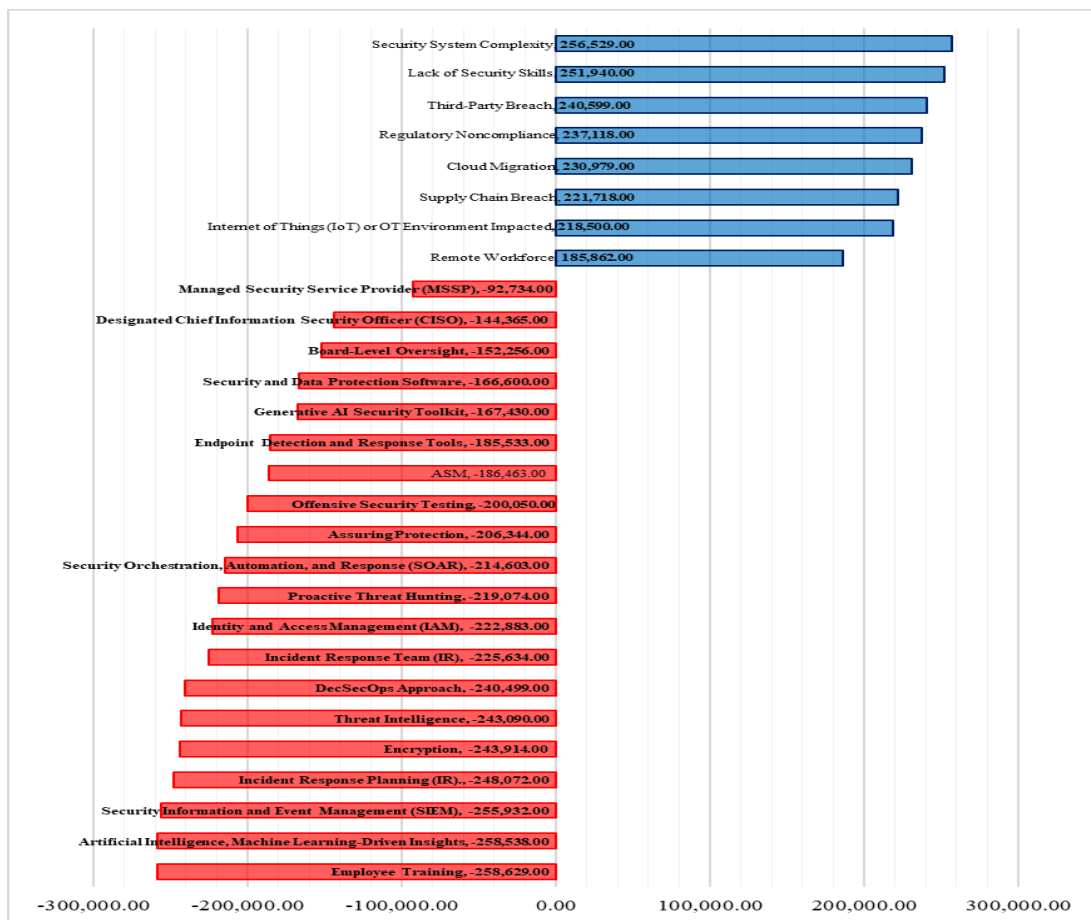


Figure 1. Overview of the impact of factors on the average amount of increase and decrease in the costs of unauthorised access to confidential data

Source: Authors based on data (IBM Corporation, 2024).

Figure 1 shows that employee training, the use of software solutions supported by artificial intelligence technology and machine learning insights are key factors that have a mitigating effect on the average cost of unauthorised access to confidential data, while the complexity of the security system, the lack of security skills, and unauthorised access and illegal use of confidential data by related parties, affect the growth of costs.

The International Monetary Fund (2024) indicates that macro-financial stability is threatened by the impact of cyber incidents and attacks, including the leakage of confidential data and the rapid materialisation of risks when key institutions in critical infrastructure are compromised (Vidović et al., 2024).

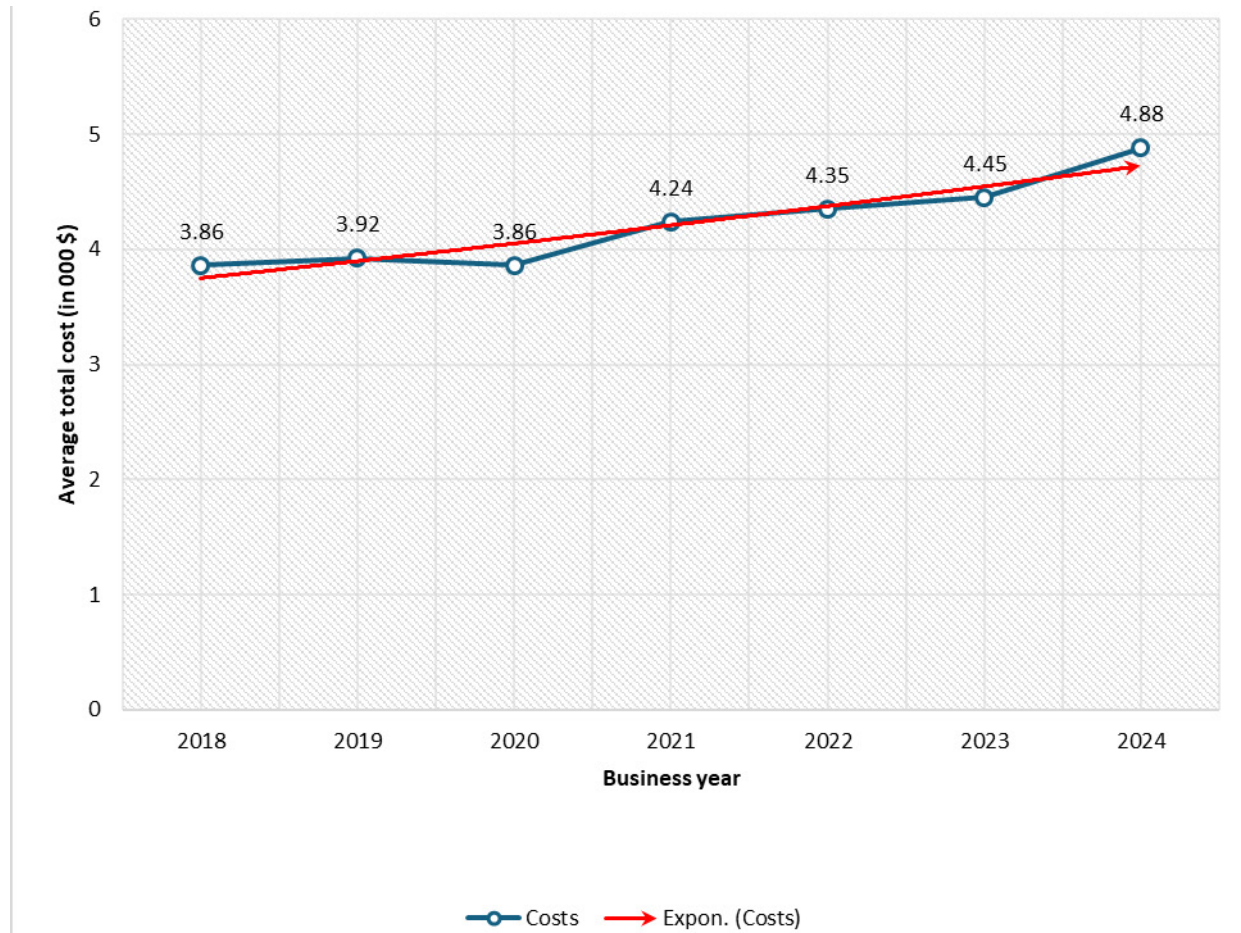


Figure 2. The trend of increasing costs of data breach incidents in cyberspace

Source: Authors based on data (IBM Corporation, 2024).

#### 4. Analysis of financial indicators of costs and damages

Econometric analysis suggests that digitalisation and geopolitical tensions significantly increase the risk of cyber incidents (International Monetary Fund, 2024). Based on an extensive study of available data from previous empirical research, literature, news articles, and official databases of international institutions reporting on cyberattacks, the analysis identified the damage caused by them. In this segment of the research, the focus was given to the analysis of cyber attacks and the leakage of confidential data, as well as the damage caused by this type of attack, which has long-term socio-financial consequences, both for the organisation, i.e. the business entity whose digital assets and personal and business data information were compromised, and for third parties outside the employees and the organisation itself, such as clients, contractors, suppliers and all dependent parties and actors in the economic chain.

Figure 3 illustrates a classification of the damage caused and the consequences of the aforementioned types of cyberattacks, encompassing economic, physical, and digital threats, as well as social, reputational, and psychological impacts.

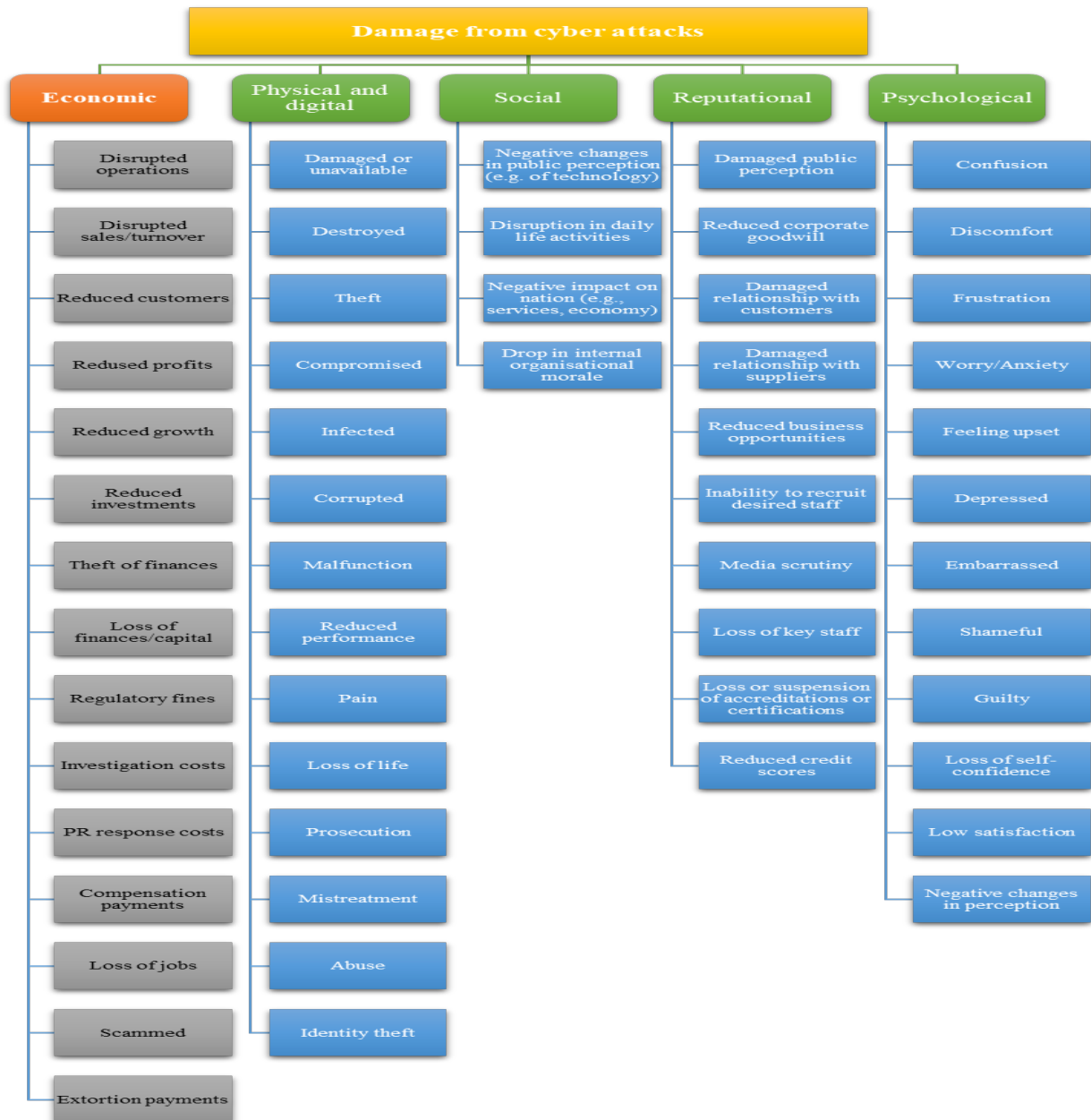
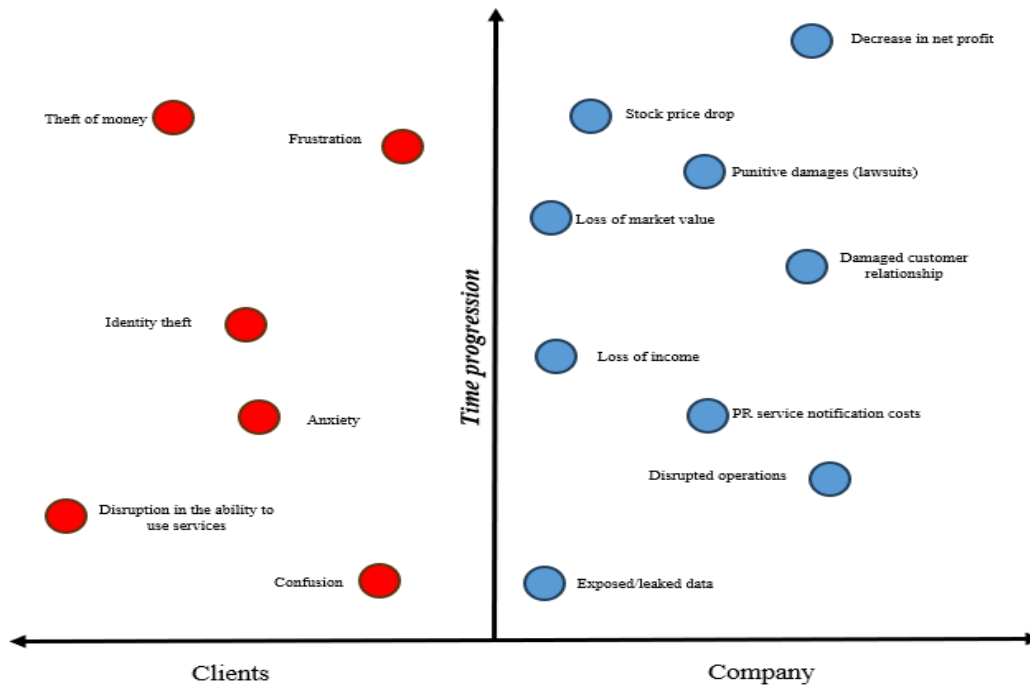


Figure 3. Classification of damages caused by cyber attacks on a business entity

Source: Authors based on data (Agrafiotis et al., 2018).

Some authors (Agrafiotis et al., 2018) define cyber damage as damage that occurs as a direct result of an attack carried out in whole or in part through digital infrastructures and the information, devices, and software applications that comprise them. The research problem was therefore approached in a multidisciplinary manner by creating an econometric model to understand the economic segment of cybersecurity, taking into account the genesis of information about cyber incidents and attacks, as well as their impact and relationship to the dynamics of development of other entities in cyberspace.

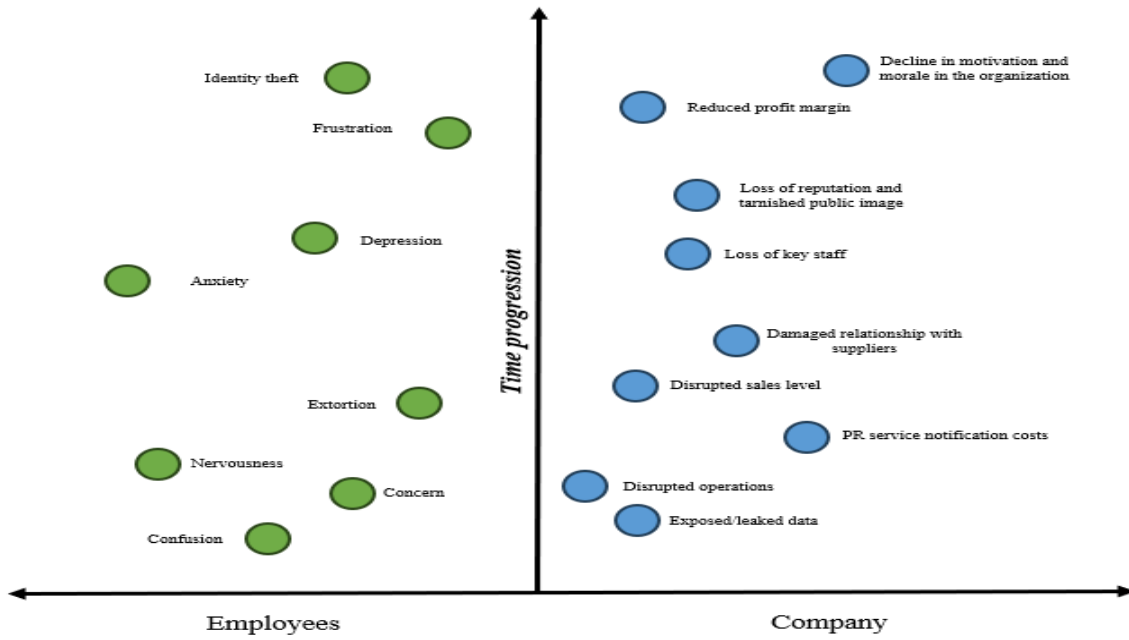
The extent of the asymmetry between costs, revenues and their actual values and the categories of financial damage assessment (direct and indirect), the consequences from an economic and social perspective, with the vector methodology and the type of cyber incident or attack in relevant case studies in the time interval from 2009 to 2024 were taken into account.



**Figure 4.** *Distribution and spread of damage after the cyberattack on the Sony Playstation Network in 2011*

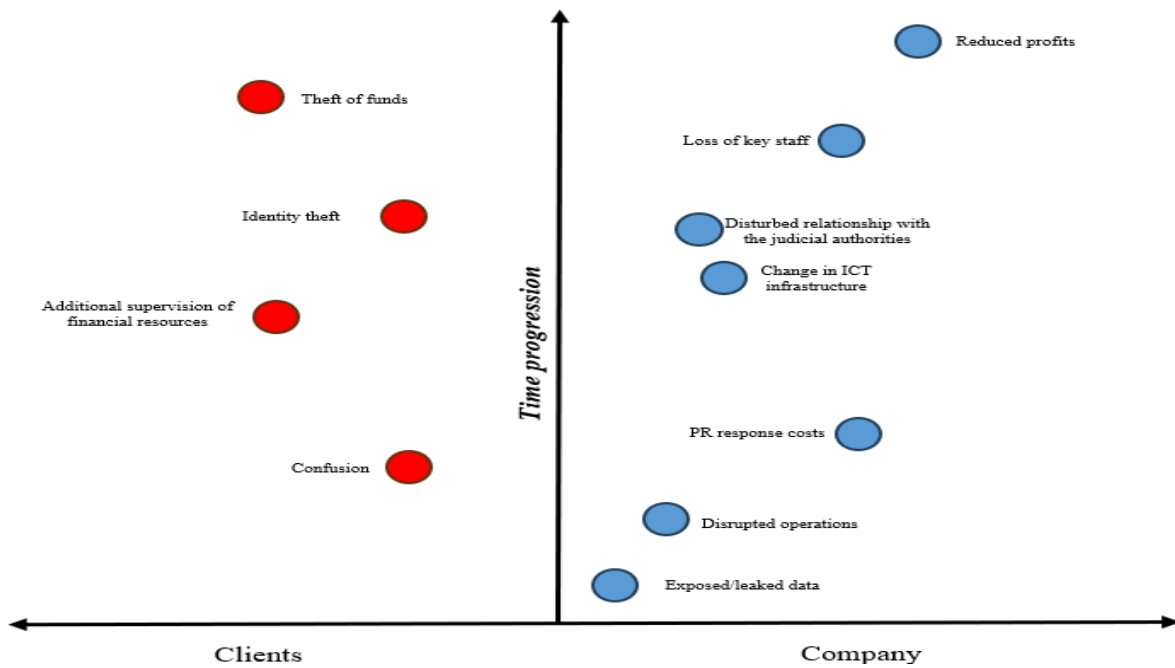
Source: Authors based on data (Sherr & Wingfield, 2011; Agrafiotis et al., 2018; Jørgensen, 2018; Quander & Janeja, 2021).

What stands out as important in the monetisation of damage and consequences is that a cyber incident on a legal entity (company, enterprise, banking system, etc.) has significant impacts on supply chains, suppliers, and directly on the object of the attack itself in the form of fluctuations in market value on the stock market when software vulnerabilities are discovered. When customer data is leaked, there is a noticeable short-term effect on share prices in financial markets. Still, there are also cases of cyber incidents where there is no direct financial damage to either companies or customers, such as the example of a DoS cyber attack on a type of data that is not confidential in nature. Still, they do have effects on the growth of the investment segment of expenditure for the technical and technological development of the entity's cybersecurity tools. Ultimately, only in cases where a cybersecurity breach in cyberspace incidents affects the confidentiality, availability or integrity of data does it have a financial impact on the company. The qualification of damages and consequences caused by cyber incidents and attacks is a specific mapping of key types and subtypes of damage (Chin, 2024). As suggested by Agrafiotis et al. (2018), a key feature and characteristic of damages and consequences in cyberspace is the domino and cascading effect of their spread, where it is essential to identify the sequences of the spread of different types of damage caused during cyberattacks and incidents. By applying the damage classification, case studies of cyber attacks in this segment of the research were processed, shown in graphs 4, 5, 6 and 7, in which we observe the distribution of impacts and the spread of damage.



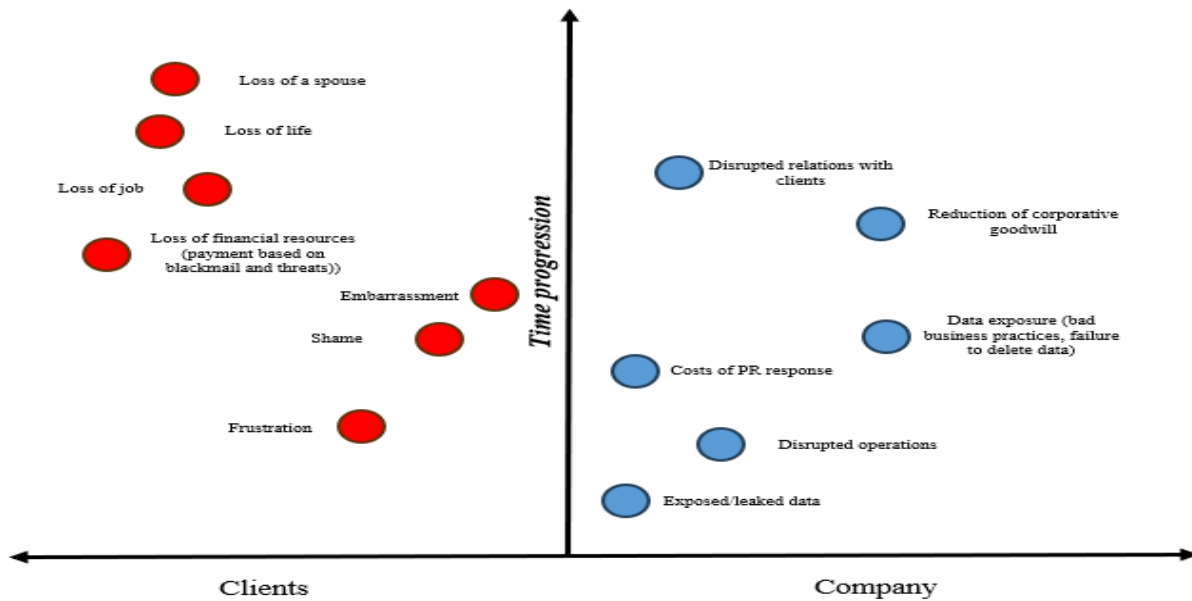
**Figure 5.** Distribution of impact and spread of damage following the cyberattack on Sony Pictures Entertainment in 2014

Source: Authors based on data (Dhillon, 2015; Ismail, 2017; Agrafiotis et al., 2018; Lis & Mendel; Steinberg et al., 2021; Muniandy et al., 2024).



**Figure 6.** Impact distribution and damage spread following the cyberattack on J.P. Morgan Chase in 2014

Source: Authors based on data (Dhillon, 2015; Agrafiotis et al., 2018)



**Figure 7.** *Distribution of impact and spread of damage after the cyberattack on Ashley Madison in 2014*

Source: Authors based on data (Agrafiotis et al., 2018).

Attacks involving the theft of personal financial information are associated with adverse stock market reactions, reduced sales growth for large firms and retailers, increased leverage, deterioration of financial health, and reduced investment in the short term (Kamiya et al., 2018) and result in long-term socioeconomic consequences (Seng et al, 2024), and the resulting costs are related to the confidentiality of compromised data, the criticality of services at risk of disruption, and the financial assets of the target of the attack (Cobos, 2024). Cybersecurity threats have a significant impact on the financial stability of organisations. The costs arising from cyber incidents are diverse.

Direct costs include the engagement of cybersecurity professionals, legal advisors, and investigators involved in incident management, recovery, and remediation.

Indirectly, cyberattacks cause significant disruptions, resulting in substantial revenue losses. Downtime disrupted workflows and reduced productivity, leading to increased operating costs and missed business opportunities. Ransomware attacks further increase financial losses, as organisations often have to pay a ransom to regain access to their data. Additionally, non-compliance with data protection laws can result in regulatory fines, further increasing the financial burden that organisations must bear following cyber incidents. A systematic presentation of analysed case studies that correlate with a relevant sample of cyber incidents and attacks on individuals and legal entities, government agencies and individual countries of the world, international companies, large, medium and small enterprises, financial institutions and critical infrastructure in the time interval of the last 15 business years, i.e. in the period from 2009 to 2024. The research of the above paid special attention to the type and methodology of the attack, with the impact it caused, and additionally, direct and indirect costs were determined using econometric and statistical methods as an integral part of the total financial damage and the cause-and-effect relationship from the attacking entity to social and economic entities.

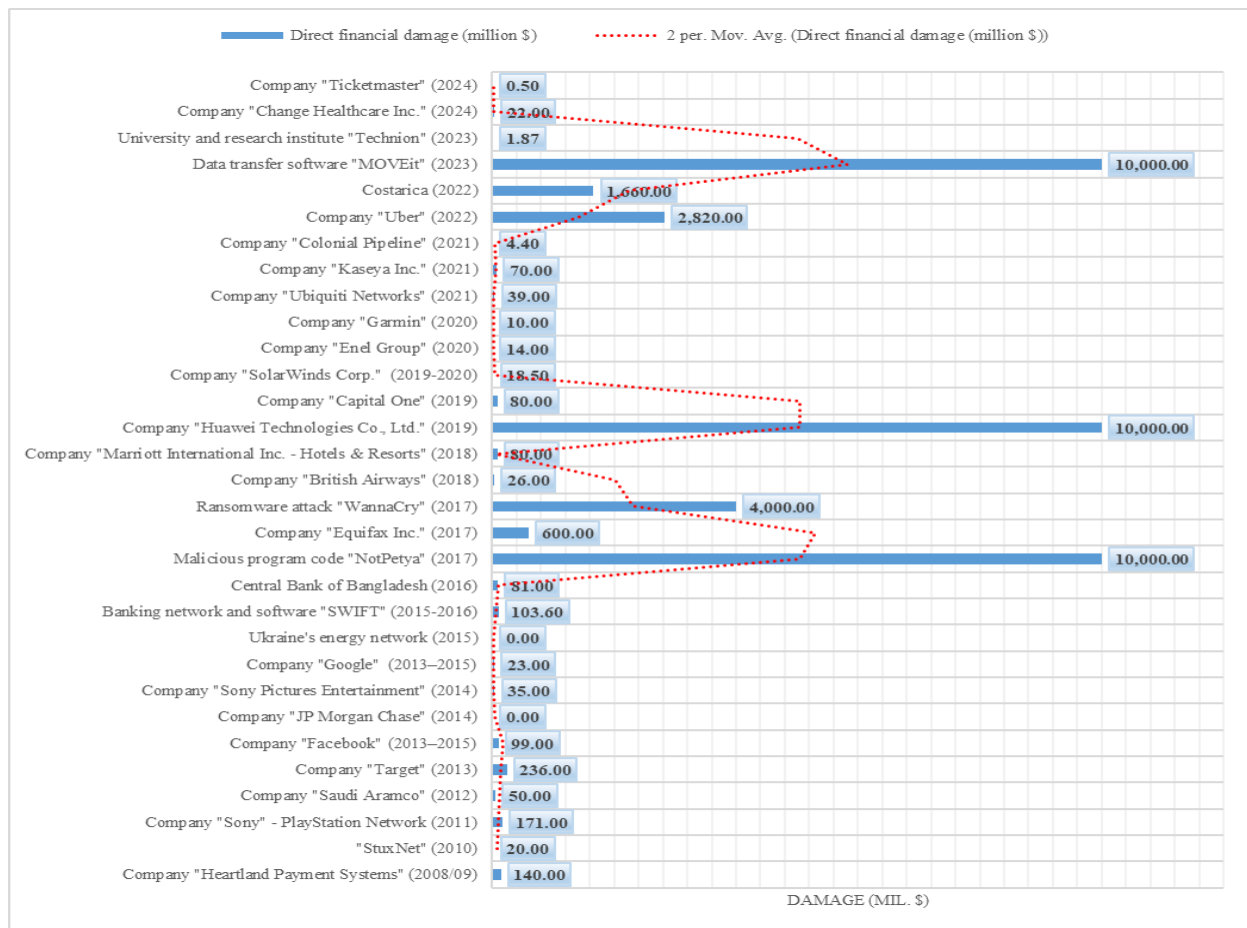


Figure 8. Direct financial damage caused by cyber-attacks and incidents in the analysed sample of case studies in the interval 2009-2024. business year

Source: Authors' calculation

## 5. Future challenges in the economic domain of cyber security

Individuals, companies, and entire nations strive to harness the power of technology to drive economic growth, enhance public services, and improve the quality of life; however, in doing so, they face increased risks associated with cyber threats. In this context, as Cobos (2024) notes, cybersecurity is crucial for socio-economic progress.

Cybersecurity is key to the inclusive and sustainable growth of nations. Estimates (Cobos, 2024) suggest that a developing country that reduces its cyber incidents from the top to the bottom quartile of the distribution could see a 1.5% increase in GDP per capita. Therefore, it is essential to develop effective measures to prevent and mitigate cyber risks by anticipating the economic consequences of cybersecurity breaches (Zadorozhnyi et al., 2021). It is important to diversify the economic causal flows that arise from established regularities and are reflected in the established trend of exponential growth in costs for finding an appropriate solution for the protection of cyber-information and computer infrastructure, where global IT companies are entering, which also contribute to building a relevant market for cyber-protection products, followed by growth in the insurance sector against cyber incidents and attacks, which directly confirms the need for capital investments in this segment (Kuzior et al., 2022). By addressing identified vulnerabilities and implementing recommended strategies, stakeholders can better protect global trade systems from the evolving cyber threat landscape, ensuring a safer and more resilient economic future (ThankGod, 2024). What the research has found, and which is further discussed in the conclusions of the World Economic Forum (2024), is that there is a growing cyber inequality between organisations, legal entities and individuals that are resilient to cyber threats and those that are not.

Good economic practices have been established, and proactive measures are being taken for the sustainable construction and development of cybersecurity (Fotis, 2024), to which this research also refers, and which include investment activities in new and advanced security technologies, proactive risk management with the implementation of regular security audits and assessments to identify vulnerabilities in systems and networks (Lee, 2021), both of business entities in the private and public sectors (Thakur, 2024). They are based on prioritising employee training and educational programs (George et al., 2024), systematic and collegial cooperation and collaboration, mutual sharing of information on cybersecurity of state authorities and other economic actors (Sunny, 2024) given that it is a shared responsibility (International Chamber of Commerce, 2024), as well as compliance with strong regulatory standards (Dremluga et al., 2021) that are harmonised (Putnik et al., 2022), development of incident response plans, investment activities in cybersecurity and continuous implementation of solutions for monitoring and detecting anomalous activities before they develop into a cyber incident or attack (Jimmy, 2024), and it is precisely this proactivity and adaptability to new challenges that ensure continued integrity and financial stability at the national, and consequently, global level level.

Cyberattacks also present an opportunity to reassess defence mechanisms and resource mobilisation capabilities (Jeimy & Cano, 2023) amid the instability they create. Although proactive security measures can be expensive, such costs are negligible compared to the financial consequences of cyberattacks (World Economic Forum, 2025). Taking into account economic parameters, the adequate establishment of cybersecurity strategies can minimise the exposure of systems and computer networks to risk (Fielder et al., 2018), provided that the right investment actions are taken to achieve a higher level of security.

## **6. Conclusion**

Rapid technological growth, while benefiting many in terms of access, innovation, and collaboration, also creates systemic inequalities in the global cybersecurity economy and challenges the pronounced disparity between the cyber resilience capabilities of the organisations that comprise its markets (World Economic Forum, 2024). The research confirmed the hypothesis that cyberattacks impose significant costs on the economy and broader society, affecting the macroeconomic stability of nations. This was evident in the case of Costa Rica in 2022, where a 2.4% loss of GDP was incurred. The average unit and aggregate costs of cyber incidents and attacks have an increasing trend in the healthcare and financial sectors of critical infrastructure, as well as in small and medium-sized business entities, especially in the wake of the COVID-19 pandemic and the Russian-Ukrainian conflict. It has been established that the accumulation of losses with long-term socio-financial consequences is based on the characteristics of indirect costs, which are most noticeable in sectors that are most financially, technically and operationally interconnected. At the same time, the most vulnerable are those sectors whose databases contain large sets of confidential data on consumers and clients, whose business is based on the provision of critical social services and which possess significant financial assets.

Empirical evidence (Cobos, 2024) indicates numerous adverse effects of cyberattacks from an economic perspective, including increased cash flow retention, reduced stakeholder and shareholder equity, reduced corporate bond ownership, reduced sales of goods, products, commodities and services, negative returns on financial markets and reduced stock prices, reduced investment in research and development, disruption and spread of losses through supply chains, economic losses to customers, operational disruptions to national and international trade flows, devastation of a business entity's reputation and brand, and erosion of trust in the digital economy.

It is essential to view cybersecurity as an economic issue, which is significant for human development in the digital age and which represents a collective responsibility. Therefore a secure cyberspace is a competitive advantage and a moral imperative, key to achieving the full potential of digital technologies and paving the way for inclusive and sustainable development in the digital age in which cyber threats are deterred, detected promptly and neutralised.

## 7. References

1. Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1).
2. Bederna, Z. and Szádeczky, T. (2023) 'Managing the financial impact of cybersecurity incidents', *Security and Defence Quarterly*, 41(1). Retrieved from: doi: 10.35467/sdq/159625.
3. Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Congressional Research Service documents, CRS RL32331 (Washington DC), 2.
4. Chin, K. (2024). The Impact of Cybercrime on the Economy, UpGuard, Retrieved from: <https://www.upguard.com/blog/the-impact-of-cybercrime-on-the-economy>.
5. Cobos, E.V. (2024). *Cybersecurity economics for Emerging Markets*. Washington, DC: World Bank. Retrieved from: doi:10.1596/978-1-4648-2120-2.
6. Cobos, V., Belen., E., Selcen, C. (2024). A Review of the Economic Costs of Cyber Incidents. Washington, D.C.: World Bank Group. Retrieved from: <http://documents.worldbank.org>.
7. Cvetković, V., Sudar, S., Ivanov, A. (2024). Harmonisation of Soft Power and Institutional Skills: Montenegro's Path to Accession to the European Union in the Environmental Sector. *International Journal of Disaster Risk Management*, 6(1), 41–74.
8. Dhillon, G. (2015). What to do before and after a cybersecurity breach. American University, Washington, DC, Kogod Cybersecurity Governance Center.
9. Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk assessment uncertainties in cybersecurity investments. *Games*, 9(2), 34.
10. Fotis, F. (2024). Economic Impact of Cyber Attacks and Effective Cyber Risk Management Strategies: A light literature review and case study analysis. *Procedia Computer Science*, 251, 471-478.
11. George, A. S., Baskar, T., & Srikanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, 2(1), 51-75. Retrieved from: <https://doi.org/10.5281/zenodo.10639463>.
12. IBM Corporation (2024). Cost of a Data Breach Report. Retrieved from: <https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec>.
13. International Monetary Fund (2024). Global Financial Stability Report, The Last Mile: Financial Vulnerabilities and Risks.
14. International Chamber of Commerce (2024). Protecting the cybersecurity of critical infrastructure and their supply chains.
15. International Telecommunication Union (2024). Global Cybersecurity Index 2024, 5<sup>th</sup> Edition. Telecommunication Development Bureau, Switzerland. Retrieved from: [https://www.itu.int/dms\\_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf](https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf).
16. Ismail, M. (2017). Sony Pictures and the U.S. Federal Government: A Case Study Analysis of the Sony Pictures Entertainment Hack Crisis Using Normal Accidents Theory, University of Southern Mississippi. Retrieved from: <https://aquila.usm.edu>.
17. Issayevaa, G. K., Zhussipovaa, E. E., Aitymbetovaa, A. N., Kuralbayevab, A. S., & Abdykulovaa, D. B. (2023). The Impact of Cybersecurity Breaches on Firm's Market Value: The Case of the USA. Retrieved from: <https://doi.org/10.51176/1997-9967-2023-4-200-219>.
18. Jeimy, J., Cano, M. (2023). Flexi-a conceptual model for enterprise cyber resilience. *Procedia Computer Science*, 219, 11-19.
19. Jimmy, F. (2024). Assessing the Effects of Cyber Attacks on Financial Markets . *Journal of Artificial Intelligence General Science (JAIGS)* ISSN:3006-4023, 6(1), 288–305. Retrieved from: <https://doi.org/10.60087/jaigs.v6i1.254>.
20. Jørgensen, E. U. (2018). The stakeholder attributions of corporate crisis responsibility following a cyber attack. Retrieved from: [https://research-api.cbs.dk/ws/portalfiles/portal/59754091/427671\\_Elisabeth\\_Jorgensen\\_digital.pdf](https://research-api.cbs.dk/ws/portalfiles/portal/59754091/427671_Elisabeth_Jorgensen_digital.pdf)

21. Kamiya, S., Kang, J.K., Kim, J. Milidonis, A. Stulz, R. (2018). What is the Impact of Successful Cyber-attacks on Target Firms?, NBER Working Papers 24409, National Bureau of Economic Research, Inc.
22. Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H., & Vasilyeva, T. (2022). Countering cybercrime risks in financial institutions: Forecasting information trends. *Journal of Risk and Financial Management*, 15(12), 613.
23. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*, 17(2), 220-239. Retrieved from: doi:10.14254/2071-8330.2024/17-2/12.
24. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659-671. Retrieved from: <https://doi.org/10.1016/j.bushor.2021.02.022>.
25. Lis, P., Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. *Economics and Business Review*, Vol. 5 (19), No. 2, 2019: 24-47. Retrieved from: DOI: 10.18559/ebr.2019.2.2.
26. Onunka, O., Alabi, A. M., Okafor, C. M., Obiki-Osafiele, A. N., Onunka, T., Daraojimba, C. (2023). Cybersecurity in US and Nigeria banking and financial institutions: review and assessing risks and economic impacts. *Acta Informatica Malaysia*, 7(1): 54-62. Cybersecurity Risk Assessment in Smart City. Retrieved from: DOI: <http://doi.org/10.26480/aim.01.2023.54.62>.
27. Putnik, N. (2022). *Cyber War and Cyber Peace*, Belgrade: Akademska misao: University, Faculty of Security.
28. Putnik, N., Milošević, M., Cvetković, V. (2022). Ransomware as a security threat – social and criminal law aspects. *Sociological Review*, vol. LVI (2022), no. 1, pp. 328–353.
29. Ryan, E., Soderber, M. (2024). A Victim or Not? A quantitative experimental study of a cyber attack crisis' effect on public attitudes toward an organization and the organization's reputation. Department of Strategic Communication, Lund University Libraries, Sweden. Retrieved from: <http://lup.lub.lu.se/student-papers/record/9154741>.
30. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15), 6666. Retrieved from: <https://doi.org/10.3390/s23156666>
31. Schwarz, M., Marx, M., & Federrath, H. (2021). A structured analysis of information security incidents in the maritime sector. arXiv preprint arXiv:2112.06545.
32. Seng, Y. J., Cen, T. Y., bin Mohd Raslan, M. A. H., Subramaniam, M. R., Xin, L. Y., Kin, S. J., Long, M. S., Sindiramutty, S. R. (2024). In-Depth Analysis and Countermeasures for Ransomware Attacks: Case Studies and Recommendations. Retrieved from: doi: 10.20944/preprints202408.2261.v1.
33. Sherr, I., Wingfield, N. (2011). Play by play: Sony's struggles on breach. *Wall Street Journal*. Retrieved from: <https://www.wsj.com>.
34. Slavković, A., Slavković, N., Zajić, G., Kostić, S. (2023). Digital transformation, artificial intelligence and internet of things as a support for new insurance industry systems. Challenges and insurance market's responses to the economic crisis, Belgrade : University of Belgrade, Faculty of economics and business, Publishing centre, 419-438.
35. Steinberg, S., Stepan, A., Neary, K. (2021). NotPetya: A Columbia University Case Study, Columbia University: Columbia's School of International and Public Affairs (SIPA) Picer Center Digital Education Group.
36. Sunny, A. (2024). A study on financial cyber-crimes, trends, patterns, and its effects in the economy. *Addict Criminol.* 7(1):186.
37. Tarter, A. (2017). Importance of cyber security. *Community Policing-A European Perspective: Strategies, Best Practices and Guidelines*, 213-230.
38. Thakur, M. (2024). Cyber security threats and countermeasures in the digital age. *Journal of Applied Science and Education (JASE)*, 4(1), 1-20.
39. ThankGod, J. (2024). Cyber Heists and Trade Turmoil: Uncovering the Economic Impact of Cybersecurity Breaches on Global Commerce. Retrieved from: <http://dx.doi.org/10.2139/ssrn.4858710>

40. Valackienė, A., Odejayi, R. O. (2024). The impact of cyber security management on the digital economy: multiple case study analysis. *Intellectual Economics*, 18(2), 261-283. Retrieved from: doi10.13165/IE-24-18-2-02.
41. Vidović, N., Beriša, H. & Cvetković, M. V. (2024). Optimising Disaster Resilience Through Advanced Risk Management and Financial Analysis of Critical Infrastructure in the Serbian Defence Industry, *International Journal of Disaster Risk Management*, Vol. 6 (2024) No. 2, Article 12 (p. 183–199), Retrieved from: <https://doi.org/10.18485/ijdrm.2024.6.2.12>
42. Weng, Y., Wu, J. (2024). Fortifying the global data fortress: a multidimensional examination of cyber security indexes and data protection measures across 193 nations. *International Journal of Frontiers in Engineering Technology*, 6(2), 13-28.
43. World Economic Forum (2024). Global Cybersecurity Outlook 2024, Insight report. Retrieved from: <https://www3.weforum.org>.
44. World Economic Forum (2025). Global Cybersecurity Outlook 2025, Insight report. Retrieved from: <https://reports.weforum.org>.
45. Zadorozhnyi, Z. M., Muravskiy, V., Shevchuk, O., & Bryk, M. (2021). Innovative accounting methodology of ensuring the interaction of economic and cybersecurity of enterprises.