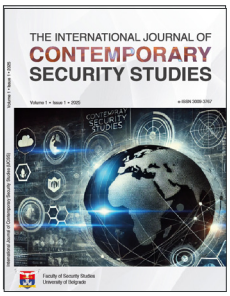
Volume 1 • Issue 2 • 2025 https://doi.org/10.18485/fb_ijcss.2025.1.2.7

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



Research article

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

Nikola Vidović[1*], Hatidža Beriša[2]

[1] University of Belgrade, Faculty of Security Studies, Belgrade, Serbia; vidovicnikola.finance@gmail.com.

[2] University of Defence, Military Academy, Belgrade – Republic of Serbia; hatidza.berisa@mod.gov.rs.

[*] Correspondence: vidovicnikola.finance@gmail.com.

Received: 02 September 2025; Revised: 20 October 2025; Accepted: 18 November 2025; Published: 30 December 2025.

ABSTRACT

The economic impacts of cyberattacks on firms, financial institutions, public authorities, and critical infrastructure between 2009 and 2024 were systematically analysed using a sample of 31 publicly documented incidents. The analysis quantified direct financial losses, indirect business disruptions, and broader socio-financial consequences. The median direct losses per incident were approximately $0.4 million, while extreme cases ranged from several hundred million to billions of dollars, in some cases equivalent to 2–2.5% of national GDP. The results confirm that cyber incidents generate multi-layered economic effects, disproportionately affecting highly interconnected sectors such as finance, healthcare, and critical infrastructure. Indirect and systemic losses – including reputational damage, legal liabilities, and erosion of consumer confidence – often exceeded the direct costs of remediation. The study highlights the importance of integrating cybersecurity into economic policy, corporate governance, and risk management strategies to mitigate these macroeconomic and firm-level vulnerabilities.

KEYWORDS

Cybersecurity, cyber attacks, economy, consequences, finance.

1. Introduction

The global economy has increasingly been shaped by digital interdependence, with financial systems, supply chains, public services, and critical infrastructure relying heavily on interconnected information and communication technologies (ICTs) (Dada, Mohammed, & Quadir, 2025; Metić, 2025; Garba & Akaan, 2025; Popović Mančević, 2025; Dada, Mohammed, Mallam, & Ajayi, 2025; Janković, Cvetković, Gačić, Renner, & Jakovljević, 2025; Vidović & Beriša, 2025). This transformation has taken place alongside growing geopolitical fragmentation, armed conflict, regulatory uncertainty, and rapid technological innovation, resulting in a complex and vulnerable economic environment (Lis & Mendel, 2019; Zadorozhnyi et al., 2021; Ryan & Söderberg, 2024; Thakur, 2024). In such conditions, economic stability has increasingly depended less on traditional macroeconomic indicators and more on the resilience of digital systems.

Vidović, N., & Beriša, H. (2025). Economic Aspects of Cyber Security: Socio-Financial Consequences of Cyber Attacks. International Journal of Contemporary Security Studies, 1(2), 105-118.

In this context, cybersecurity has emerged as a key factor in economic and financial stability. The World Economic Forum (2024) identified cyber risks as one of the most serious global threats, noting that the cybersecurity sector has been growing faster than the overall global economy. This development has reflected not only technological advances but also the increasing frequency and sophistication of cyberattacks. As more than 60% of global financial transactions are conducted in a digital environment, cyber incidents have increasingly led to direct economic losses, operational disruptions, and erosion of trust in digital and financial systems (Valackienė & Odejayi, 2024). At the same time, the widespread application of artificial intelligence, cloud computing, and blockchain technologies has increased both economic efficiency and systemic vulnerability (Slavković et al, 2023; Saeed et al., 2023; Weng & Wu, 2024) and the challenges of cybersecurity, which is precisely the consumer society as a sociological category, with its consumerization, putting it in the focus of new research (International Telecommunication Union, 2024). The expansion of user functions provided by digitalization has encouraged the development of products and services in the virtual space, emphasizes 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 (Issayevaa et al, 2023).

Cybersecurity threats and incidents in cyberspace negatively affect the market value of business entities, revenue, profit, reputation and brand, market capitalization, intangible assets, and financial policies of companies (Issayeva et al, 2023), where publicly disclosed cyber incidents are growing globally, with an annual growth rate of 21% (Cobos, 2024). The research sought to bridge this gap by applying an integrated economic analysis of cyber incidents. The main objective of the study was to examine the impact of the frequency and severity of cyberattacks on economic stability through direct financial losses, indirect business disruptions, and broader socio-financial effects. The initial hypothesis was that the increasing frequency and sophistication of cyberattacks would proportionally increase business losses and contribute to macroeconomic instability in the public and private sectors, and the research results confirmed this. Methodologically, the study employed a mixed analytical approach, including descriptive statistical analysis, econometric techniques, and comparative case analysis. The analysis is based on a sample of 31 publicly documented cyber incidents from 2009 to 2024, spanning different sectors and regions. Direct financial losses, indirect costs, firm-level performance indicators, as well as selected macroeconomic and socio-financial variables were examined, with regression and trend analyses used to assess the relationship between cyber incident characteristics and economic outcomes.

2. Financial factors and implications for cyber security

The digitalization of social activities has caused humanity to rely entirely on the reliability, security (Cvetkovic et al., 2025), and integrity that it provides, due to the efficiency of computer automation in performing everyday tasks. Every social phenomenon is accompanied by different aspects and outcomes, and, viewed generally, these effects are positive and negative. The expansion of user functions provided by digitalization 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 organizations. All of these challenges are exacerbated by a growing skills gap, which further complicates effective cyber risk management (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.Source: Authors based on data from Petit (2024).

State/Region	Agency	The basics of Cyber Incident and Attack Reporting	Type of report	Time frame
USA	CISA	CIRCIA	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
		CIRCIA - 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	ENISA	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 on ICT Systems by Financial Institutions	24 hours
	National Supervisory Authority	GDPR	Report on the violation of the personal data of the organization	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 organizations and entities operating	3-5 days
		Basic 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

Narrowing the focus to the business context, two concepts closely related to harm are "*impact*" and "*risk*. Both concepts are pervasive in economic empirical research, literature, and practice, as Agriofotis et al. (2018) point out, because they represent the activity of one or more individuals that can lead to positive or negative outcomes through cause-and-effect relationships. This characterization 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 impact as the potential harm expected to result from unauthorized actions or the 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 emphasizing 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 organizations 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 analyzing the costs of cyberattacks, IBM Corporation (2024) identified patterns in business activities that tend to reduce or increase them.

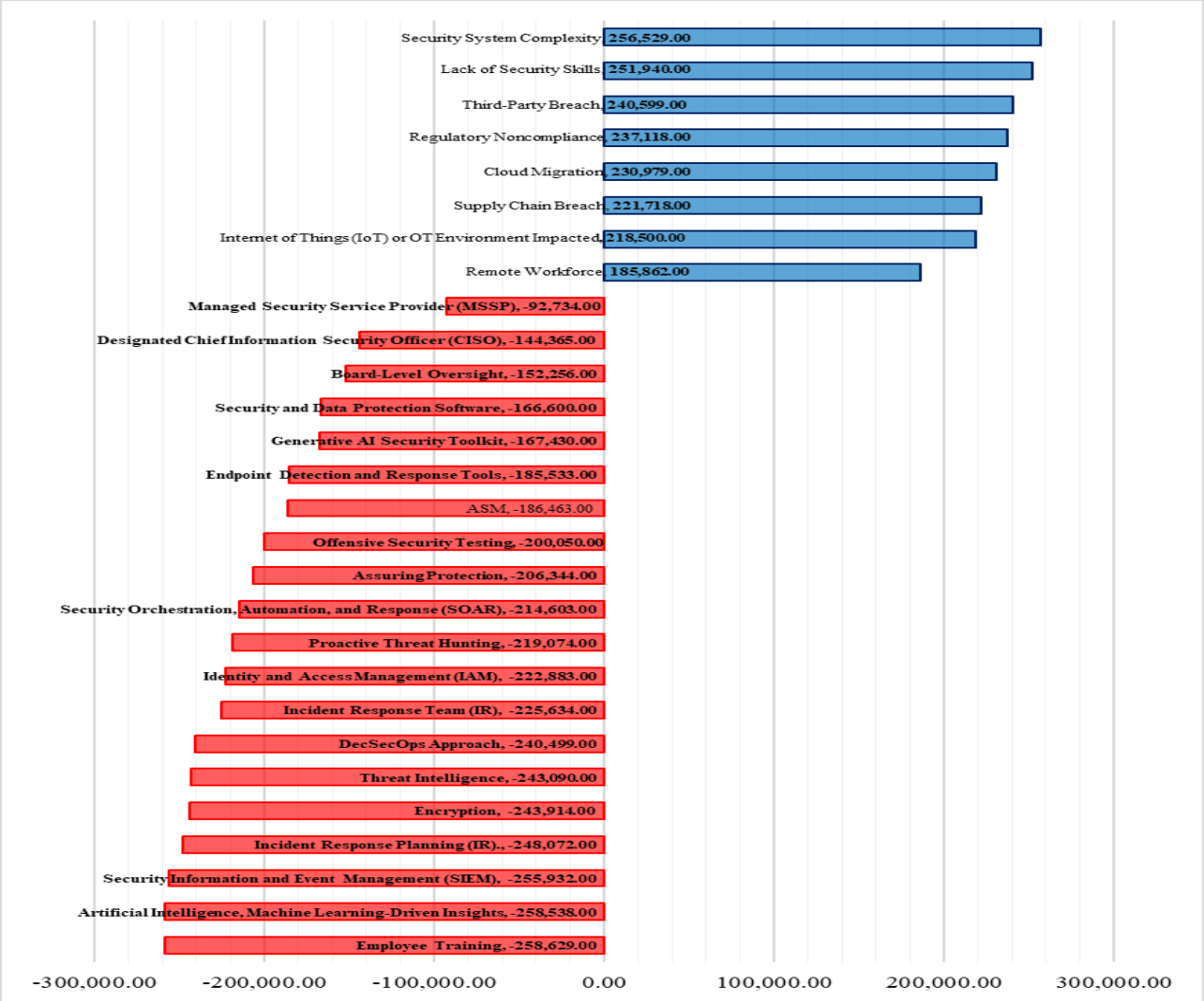


Figure 1. Overview of the impact of factors on the average amount of increase and decrease in the costs of unauthorized access to confidential data. Source: Authors based on data (IBM Corporation, 2024).

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 unauthorized access to confidential data, while the complexity of the security system, the lack of security skills, and unauthorized 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 materialization of risks when key institutions in critical infrastructure are targeted (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 digitalization and geopolitical tensions significantly increase the risk of cyber incidents (International Monetary Fund, 2024). Based on an extensive review of data from previous empirical research, the literature, news articles, and official databases of international institutions reporting on cyber attacks, the analysis identified the damage caused by cyber attacks. 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 organization, 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 organization itself, such as clients, contractors, suppliers and all dependent parties and actors in the economic chain.

Figure 3 shows a classification of the damage caused and the consequences of the above types of cyberattacks, covering economic aspects, physical and digital threats, and social, reputational, and psychological impacts.

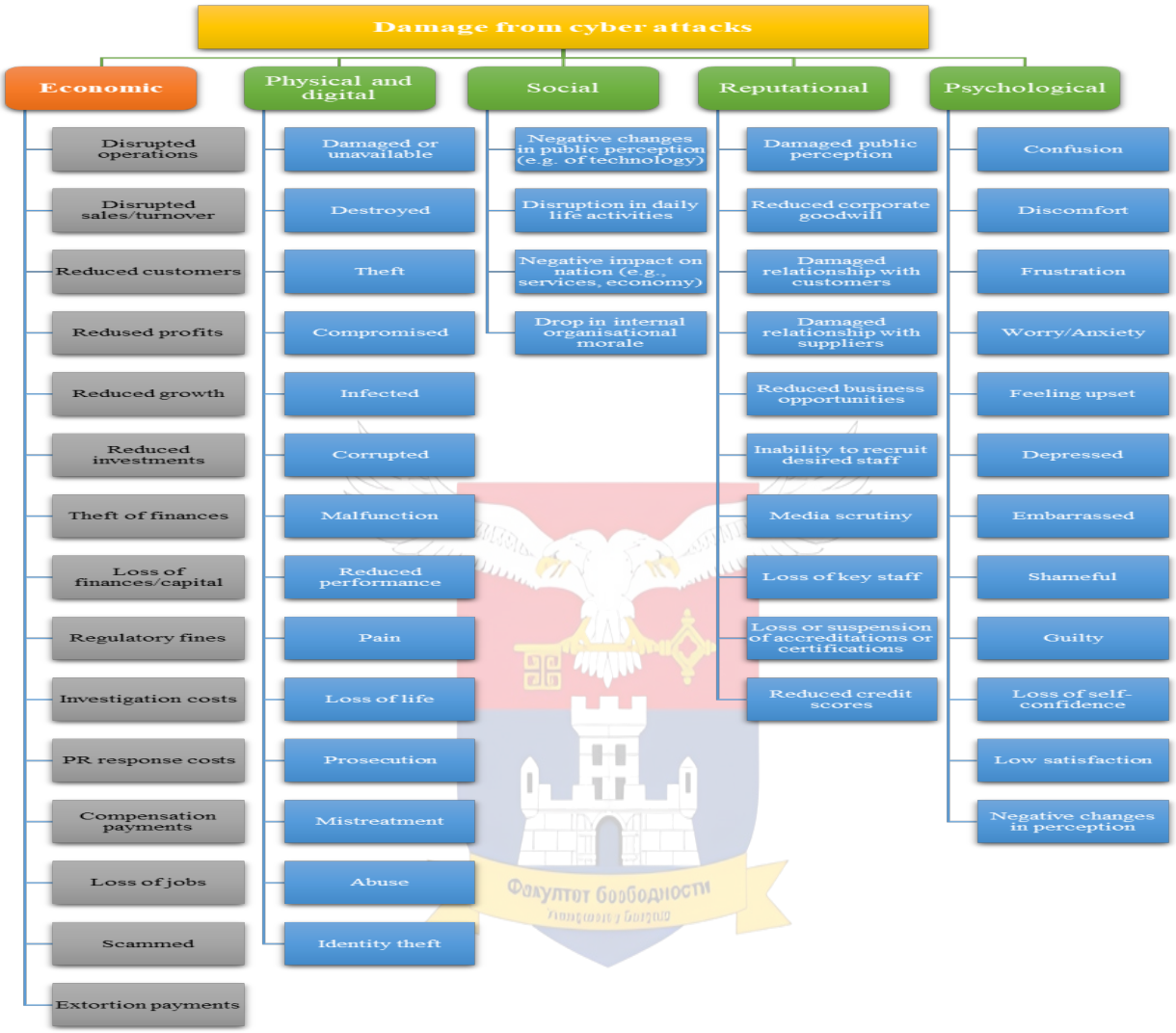


Figure 3. Classification of damages caused by cyber attacks on a business entity. Source: Authors based on data (Agrafiotis et al, 2018).

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 infrastructure and the information, devices, and software applications that comprise it. 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, their impact, and their 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.

What stands out as important in the monetization 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 on financial markets. However, there are also cases of cyber incidents in which there is no direct financial damage to either companies or customers, such as a DoS attack on data that is not confidential. However, 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 or incident in cyberspace affects the confidentiality, availability, or integrity of data does it have a financial impact on the company. The qualification of damages and consequences from cyber incidents and attacks involves a specific mapping of key types and subtypes of damage (Chin, 2024). As suggested by Agrafiotis et al. (2018), an important feature of damages and consequences in cyberspace is the domino and cascading effect of their spread, and it is important to clearly identify the sequences of spread for different types of damage caused during cyber attacks and incidents. By applying the damage classification, case studies of cyber attacks in this segment of the research were processed, as shown in Figures 4, 5, 6, and 7, which reveal the distribution of impacts and the spread of damage.

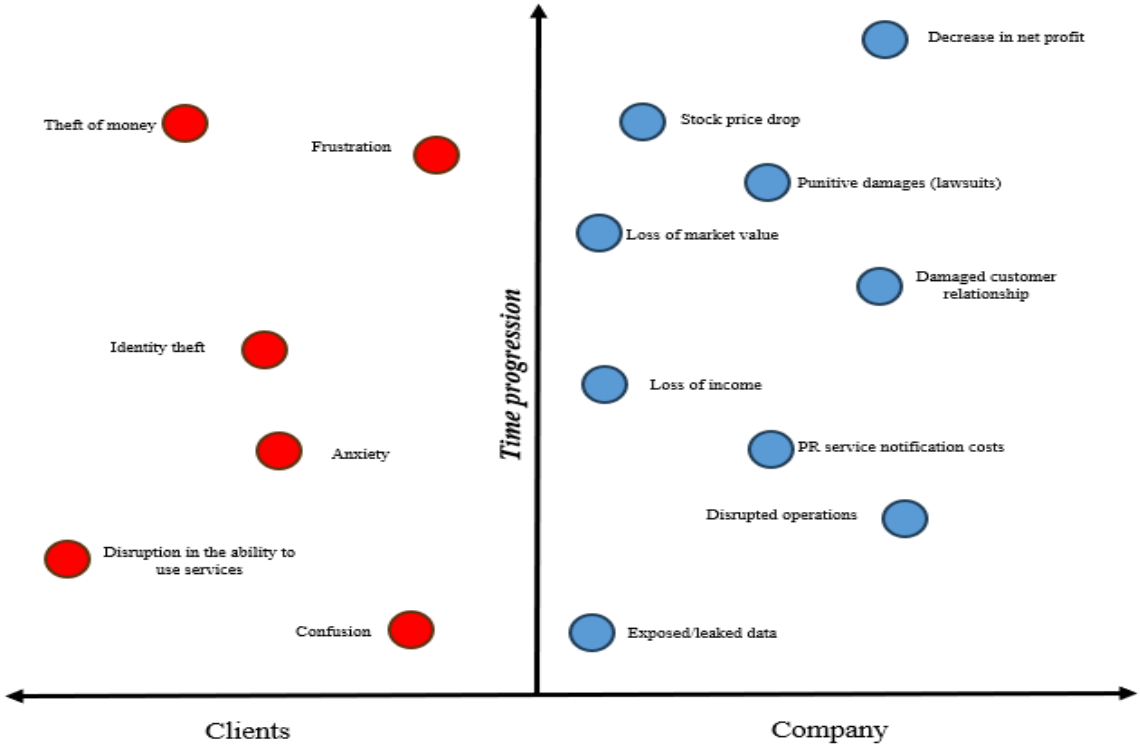


Figure 4. Distribution and spread of damage following the 2011 cyberattack on the Sony PlayStation Network. Source: Authors based on data (Sherr & Wingfield, 2011; Agrafiotis et al, 2018; Jørgensen, 2018; Quander & Janeja, 2021).

Figures 4 and 5 illustrate the changing structure of economic damage from cyber incidents within the same corporation. The 2011 attack on Sony PlayStation Network caused a gradual spread of losses from operational disruption to market and institutional levels, with indirect losses, such as reputational erosion and legal exposure, exceeding direct remediation costs estimated at US$171 million. In contrast, the 2014 incident at Sony Pictures Entertainment had a more direct and destructive economic impact, with quantifiable revenue losses of at least US$30 million and write-offs of film projects totaling US$82-US$95 million. While the first case primarily disrupted the digital platform's customer relationship and market position, the second directly affected internal business processes and organizational stability. These findings indicate that cyber risks in digitally intensive sectors are transforming from reputational and market threats to strategic threats that directly threaten revenues and operational continuity.

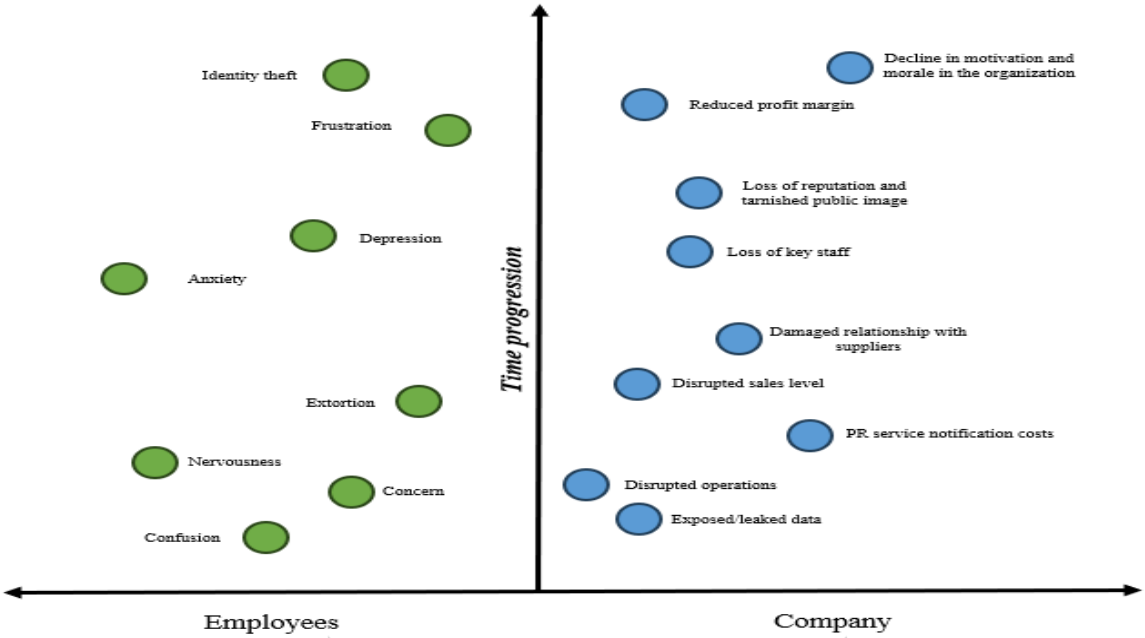


Figure 5. Distribution of impact and spread of damage following the cyberattack on Sony Pictures Entertainment in 2014. Source: auteurs, sur la base de données (Dhillon, 2015; Ismail, 2017; Agrafiotis et al., 2018; Lis & Mendel; Steinber et al., 2021; Muniandy et al., 2024).

Figure 6. Impact distribution and damage spread following the 2014 cyberattack on J.P. Morgan Chase. Source: Authors based on data (Dhillon, 2015; Agrafiotis et al, 2018)

On the other hand, Figures 6 and 7 show that serious cyber incidents may have minimal or no direct financial losses, but produce enormous systemic, regulatory, and societal effects. JP Morgan Chase incurred increased security costs (~$500 million) and a significant drop in consumer confidence, prompting measures across the financial industry. The Ashley Madison attack demonstrated that a breach of user privacy can cause collateral damage, including public scandals, lawsuits, threats, and even suicides. However, direct financial losses were not the primary outcome.

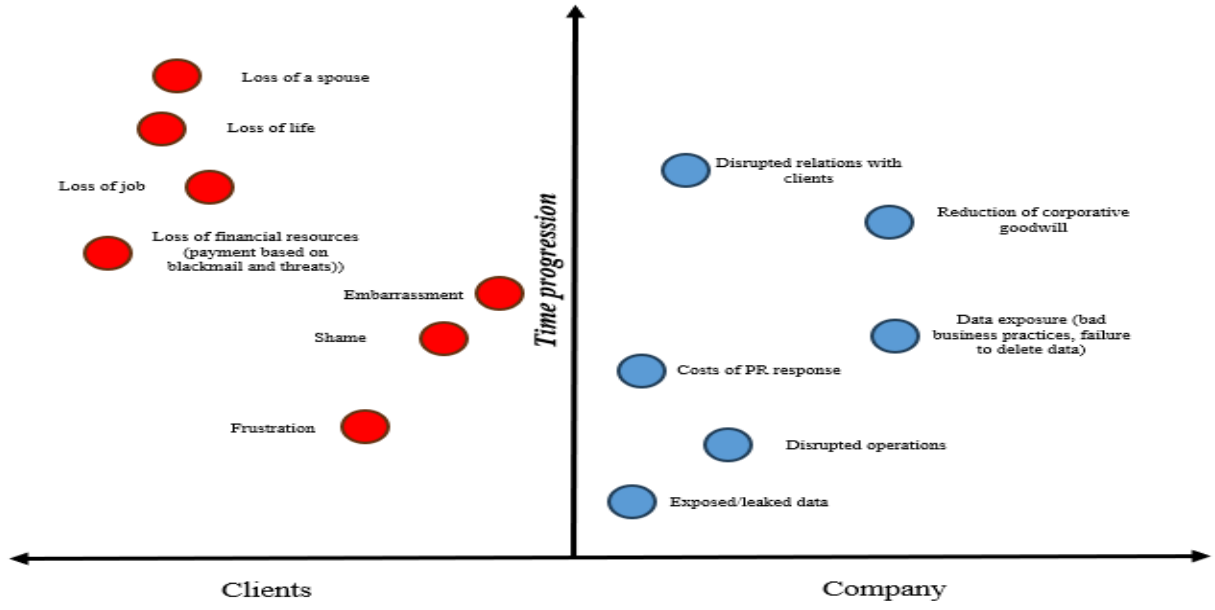


Figure 7. Distribution of impact and spread of damage after the cyberattack on Ashley Madison in 2014. Source: Authors based on data (Agrafiotis et al, 2018).

Combined, these examples highlight that the effects of cyberattacks are multi-sectoral and multi-level, with indirect and systemic losses often exceeding direct financial costs. The financial sector and critical infrastructure experience higher-than-average indirect losses, while privacy-focused platforms suffer profound reputational and societal shocks, supporting broader findings from the study on the cumulative economic and socio-financial consequences of cyber incidents. 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 significantly impact organizations' financial stability. The costs arising from cyber incidents are diverse.

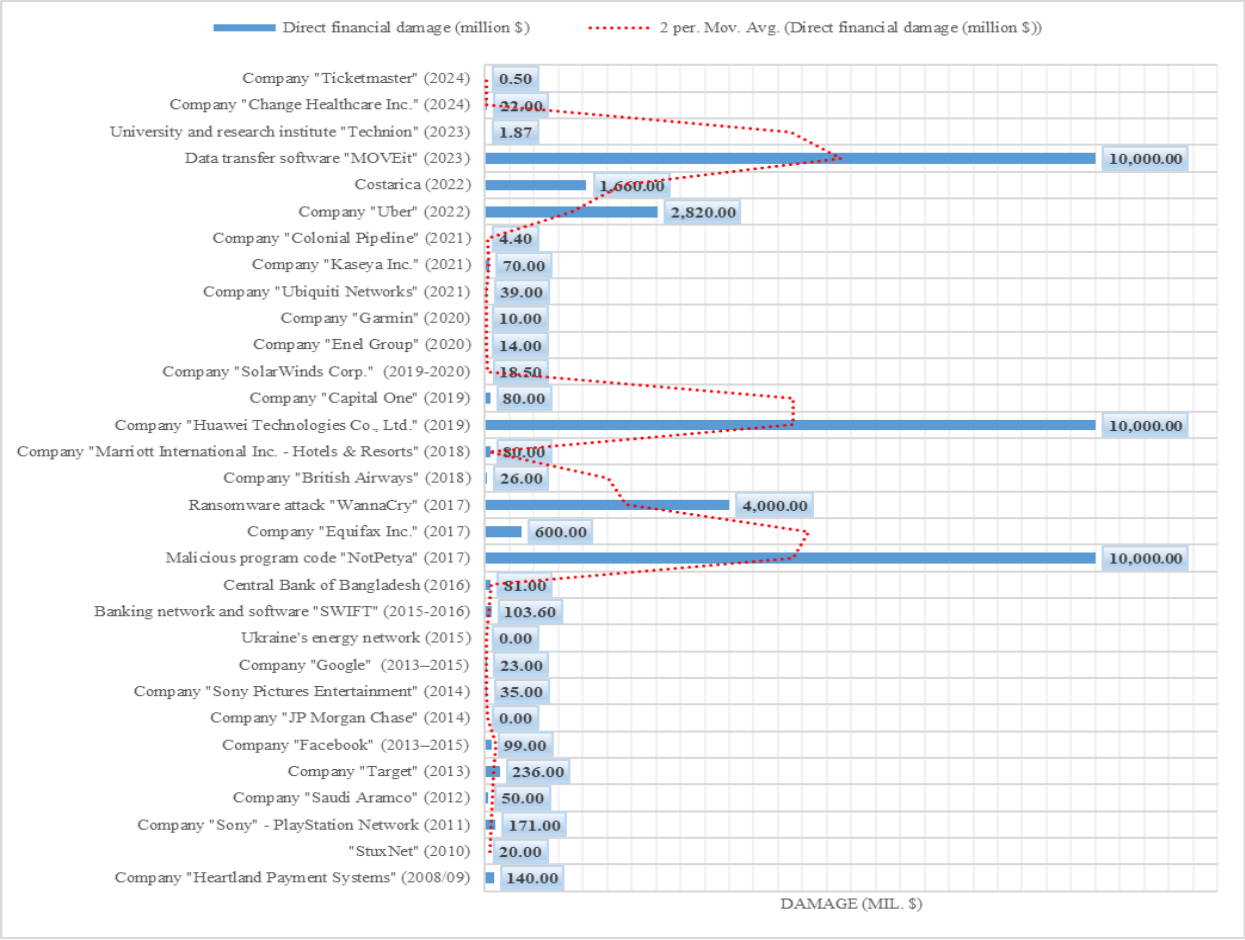


Figure 8. Direct financial damage caused by cyber attacks and incidents in the analyzed sample of case studies in the interval 2009-2024. business year. Source: Author's calculation

Based on the analyzed data, the average direct damage per cyber incident was approximately $0.4 million, with three-quarters of incidents resulting in losses below $2.8 million (International Monetary Fund, 2024). However, the distribution is highly skewed, as some incidents cause losses in the hundreds of millions of dollars or, in some cases, accumulate financial damage of several million, which can threaten the liquidity and solvency of business entities. Direct costs include engaging security experts, legal advisors, and researchers in the recovery and treatment process. Indirect losses arise from work interruptions, shifts in business flow, reduced productivity, missed opportunities, and ransom payments in the event of ransomware attacks, as well as possible regulatory penalties for non-compliance with data protection laws. A systematic analysis of 31 cyber incidents from 2009 to 2024, covering various sectors – from government agencies and multinational companies to financial institutions, direct measures, and critical infrastructure. Economic and statistical methods create cumulative economic and socio-financial effects that spread from the immediate targets of the incident to the broader economic and social environment.

5. Future challenges in the economic domain of cybersecurity

Individuals, companies, and entire nations aim to harness the power of technology to drive economic growth and improve public services and quality of life, but in doing so, they face increased risks from cyber threats. In this context, as Cobos (2024) points out, cybersecurity is essential 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 important to develop effective measures to prevent and eliminate 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 organizations, 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 prioritizing 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 (Dremliuga et al, 2021) that are harmonized (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 ensures continued integrity and financial stability at the national, and consequently, global level. Level.

Cyberattacks also present an opportunity to reassess their defense mechanisms and resource mobilization capabilities (Jeimy & Cano, 2023) amid the instability they present. 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 effective establishment of cybersecurity strategies can minimize the exposure of systems and computer networks to risk (Fielder et al., 2018), only with the right investment actions to achieve a higher level of security.

6. Conclusion

Rapid technological growth, while benefiting many in terms of access, innovation, and even collaboration, also creates systemic inequalities in the global cybersecurity economy and challenges the pronounced disparity between the cyber resilience capabilities of the organizations that make up its markets (World Economic Forum, 2024). The study confirmed the hypothesis that cyberattacks have a significant, measurable macroeconomic impact, threatening national economic stability. Empirical data showed that direct and indirect losses can exceed initial damage estimates, and the sectors most technically, financially, and operationally interconnected are most affected: finance, healthcare, small and medium-sized enterprises, and platforms that process large volumes of sensitive user data. The cumulative effects manifest themselves through long-term socio-financial consequences, including loss of trust, reputational damage, and regulatory oversight.

Based on these findings, the study highlights the need to integrate cyber risks into economic policy, budget planning for prevention and response, and the development of strategic frameworks for risk management at

the sectoral and national economic levels. A secure and resilient digital space is a competitive advantage and a prerequisite for sustainable economic development in the digital era.

Limitations of the study include reliance on secondary public data sources and uneven availability of cyber incident reports globally, which may affect the accuracy of the estimates. Future research should focus on modeling economic costs by sector, conducting regional comparisons, and developing dynamic models that integrate the direct, indirect, and socio-financial impacts of cyberattacks.

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. M., Aleksov, B., Renner, R., Gačić, J., Ivanov, A., & Milašinović, S. (2025). Community-based disaster risk reduction: Overcoming barriers to build stronger communities. International Journal of Disaster Risk Management, 7(2), 1.
8. Dada, K. S. J., Mohammed, H. A., & Quadir, R. O. (2025). Disaster risk management in academic institutions: An assessment of preparedness and recovery at Kashim Ibrahim Library, Nigeria. International Journal of Contemporary Security Studies, 1(1), 1–15.
9. Dada, K. S. J., Mohammed, H. A., Mallam, D., & Ajayi, E. O. (2025). Security of information resources in Federal College of Education libraries in Northwest Nigeria. International Journal of Contemporary Security Studies, 1(1), 85–98.
10. Dhillon, G. (2015). What to do before and after a cybersecurity breach. American University, Washington, DC, Kogod Cybersecurity Governance Center.
11. Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk assessment uncertainties in cybersecurity investments. Games, 9(2), 34.
12. 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.
13. Garba, T. M., & Akaan, R. (2025). The Socioeconomic and Psychological Implications of Polygamy: A Quantitative and Qualitative Analysis Concerning Disaster Risk Reduction and Management (DRRM) in Nigeria. International Journal of Contemporary Security Studies, 1(1), 25–34.
14. George, A. S., Baskar, T., & Srikaanth, 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.
15. IBM Corporation (2024). Cost of a Data Breach Report. Retrieved from: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec.
16. International Chamber of Commerce (2024). Protecting the cybersecurity of critical infrastructure and their supply chains.

17. International Monetary Fund (2024). Global Financial Stability Report, The Last Mile: Financial Vulnerabilities and Risks.

18. International Telecommunication Union (2024). Global Cybersecurity Index 2024, 5th 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.

19. 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.

20. 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.

21. Janković, L., Cvetković, V. M., Gačić, J., Renner, R., & Jakovljević, V. (2025). Integrating psychosocial support into emergency and disaster management and public safety: The role of the Red Cross of Serbia. International Journal of Contemporary Security Studies, 1(1), 99–124.

22. Jeimy, J., Cano, M. (2023). Flexi-a conceptual model for enterprise cyber resilience. Procedia Computer Science, 219, 11-19.

23. 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.

24. 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

25. Kamiya, S., Kang, J.K., Kim, J., Milidonis, A., Stulz, R. (2018). What is the Impact of Successful Cyberattacks on Target Firms?, NBER Working Papers 24409, National Bureau of Economic Research, Inc.

26. 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.

27. 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.

28. 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.

29. 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.

30. Metić, A. (2025). The Significance and Role of Police Officers in Building the School as a Safe Environment for All Students. International Journal of Contemporary Security Studies, 1(1), 17–24.

31. 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.

32. Popović Mančević, M. (2025). Non-Traditional Roles of Military Actors: NATO's Engagement in Natural Disaster Response. International Journal of Contemporary Security Studies, 1(1), 75–84.

33. Putnik, N. (2022). Cyber War and Cyber Peace, Belgrade: Akademska misao: University, Faculty of Security.

34. 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.

35. 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 on the organization's reputation. Department of Strategic Communication, Lund University Libraries, Sweden. Retrieved from: http://lup.lub.lu.se/student-papers/record/9154741.

36. 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

37. Schwarz, M., Marx, M., & Federrath, H. (2021). A structured analysis of information security incidents in the maritime sector. arXiv preprint arXiv:2112.06545.

38. 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.

39. Sherr, I., Wingfield, N. (2011). Play by play: Sony's struggles on breach. Wall Street Journal. Retrieved from: https://www.wsj.com.

40. 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.

41. 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.

42. Sunny, A. (2024). A study on financial cyber-crimes, trends, patterns, and its effects in the economy. Addict Criminol. 7(1):186.

43. Tarter, A. (2017). Importance of cyber security. Community Policing-A European Perspective: Strategies, Best Practices and Guidelines, 213-230.

44. Thakur, M. (2024). Cyber security threats and countermeasures in digital age. Journal of Applied Science and Education (JASE), 4(1), 1-20.

45. 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

46. 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.

47. Vidović, N., & Beriša, H. (2025). Economic aspects of cyber security: Socio-financial consequences of cyber attacks. International Journal of Contemporary Security Studies, 1(1), 149–162.

48. 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

49. Weng, Y., Wu, J. (2024). Fortifying the global data fortress: a multidimensional examination of cybersecurity indexes and data protection measures across 193 nations. International Journal of Frontiers in Engineering Technology, 6(2), 13-28.

50. World Economic Forum (2024). Global Cybersecurity Outlook 2024, Insight report. Retrieved from: https://www3.weforum.org.

51. World Economic Forum (2025). Global Cybersecurity Outlook 2025, Insight report. Retrieved from: https://reports.weforum.org.

52. Zadorozhnyi, Z. M., Muravskyi, V., Shevchuk, O., & Bryk, M. (2021). Innovative accounting methodology of ensuring the interaction of economic and cybersecurity of enterprises.