Understanding Ransomware Through the Lens of Disaster Risk: Implications for Cybersecurity and Economic Stability

Nikola Vidović , Vladimir M. Cvetković * , Hatidža Beriša , Srđan Milašinović

Posted Date: 27 April 2025

doi: 10.20944/preprints202504.1950.v1

Keywords: ransomware; cybersecurity; disaster risk; digital economy; financial impact; critical infrastructure; cyber resilience; socio-economic consequences; risk governance; ransomware-as-a-service (RaaS)

 doi:10.20944/preprints202504.1950.v1

Article

Understanding Ransomware Through the Lens of Disaster Risk: Implications for Cybersecurity and Economic Stability

Nikola Vidović [1], Vladimir M. Cvetković [1,2,3,*], Hatidža Beriša [4] and Srđan Milašinović [5]

[1] Faculty of Security Studies, University of Belgrade, Gospodara Vucica 50, 11040 Belgrade, Serbia
[2] Safety and Disaster Studies, Chair of Thermal Processing Technology, Department of Environmental and Energy Process Engineering, Montanuniversitaet, Leoben, Austria
[3] Scientific-Professional Society for Disaster Risk Management, Dimitrija Tucovića 121, 11040 Belgrade, Serbia
[4] University of Defence, Military academy, Belgrade – Republic of Serbia, Veljka Lukića Kurjaka 1, 11000 Belgrade
[5] University of Criminal Investigation and Police Studies, Cara Dušana 196, Belgrade
* Correspondence: vmc@fb.bg.ac.rs or vladimir.cvetkovic@unileoben.ac.at

Abrstract: Ransomware has emerged as a modern digital crisis, mirroring the widespread disruptions typically associated with natural or artificial disasters. As global economies grow increasingly interconnected through digital systems, the fallout from ransomware attacks stretches far beyond mere technical breaches. These incidents lead to severe financial damage, disrupt operations, erode reputations, and contribute to broader socio-economic instability. This study adopts a disaster risk perspective to examine ransomware's wider economic and social toll, particularly its impact on critical infrastructure and public trust in institutions. Through a multi-case analysis of sixteen significant ransomware attacks between 2015 and 2025, the research highlights a recurring pattern: direct and indirect costs often compound, with impacts varying from ransom demands and halted services to reputational loss and sector-wide vulnerabilities. The rise of Ransomware-as-a-Service (RaaS) has also made these attacks more accessible and complex, deepening the threat landscape. The findings indicate an urgent need to integrate cybersecurity into broader disaster risk management strategies. Policymakers, institutions, and businesses must adopt a forward-looking approach—emphasising continuous risk evaluation, resilient digital infrastructure, and collaboration across sectors. To protect economies from escalating cyber threats, adaptive regulations and anticipatory defenses are no longer optional—they're essential.

Keywords: ransomware; cybersecurity; disaster risk; digital economy; financial impact; critical infrastructure; cyber resilience; socio-economic consequences; risk governance; ransomware-as-a-service (RaaS)

1. Introduction

In the current digital economy, over 60 percent of commercial transactions occur online, exposing cyberspace to vulnerabilities and necessitating high-quality security for optimal, transparent transactions (Valackienė & Odejayi, 2024). Insights from last year's World Economic Forum (2024) underscore that global financial stability faces threats from the rising frequency and sophistication of cyberattacks; tactics have evolved through the use of artificial intelligence, ransomware as a service, and advanced social engineering techniques, enabling attackers to bypass traditional cyber defences. This notion is further supported by various insurance companies assessing cybersecurity risks in businesses (HISCOX Group, 2024), highlighting the crucial role of cybersecurity in the global economy (Kala, 2023). More than 5. 4 billion people and countless groups and organisations actively use the internet. According to estimations and remarks from Kuzior et al. (2022,

 doi:10.20944/preprints202504.1950.v1

2024), the digital transformation market is projected to grow from $ 469. 8 billion in 2020 to $ 1. 01 trillion in the 2025 business year. It may reach up to $ 3. 9 trillion by 2027, with a compound annual growth rate of 16. 1%.

Despite the increasing literature on ransomware's technical elements, there remains a shortfall in integrated analysis connecting financial impacts to broader disaster risk perspectives (Cvetković, Renner, & Jakovljević, 2024; Jurišić & Marceta, 2024; Mokhele, 2024; Molnár, 2024; Rebouh, Tout, Dinar, Benzid, & Zouak, 2024; Umer, 2024; Vidović, Cvetković, & Beriša, 2024). Understanding the economic stability implications of ransomware and its effects on critical infrastructure and public trust is a significant research gap in the realms of cybersecurity and risk governance. While numerous studies have delved into the technical dissection of ransomware attacks, few have investigated their broader consequences on financial stability, sectoral resilience, and public trust through a holistic, disaster- centric analytical framework (Axon, Erola, Agrafiotis, Uuganbayar, Goldsmith, & Creese, 2023; Benmalek, 2024; Connolly, Wall, Lang, & Oddson, 2020; Goodell & Corbet, 2022; Molina, Torabi, Sarieddine, Bou- Harb, Bouguila, & Assi, 2022; Mott et al., 2024; Pattnaik et al., 2023; Reshmi, 2021; Wollerton, 2023; Zimba & Chishimba, 2019). This research seeks to address this gap. Given the increasing intensity, frequency, and extensive impact of ransomware attacks, these incidents lend themselves to interpretation within a disaster risk framework.

According to the United Nations Office for Disaster Risk Reduction (UNDRR), disaster risk is defined as the potential loss of life, injury, or destroyed or damaged assets that could occur to a system, society, or a community in a specific period, determined probabilistically as a function of hazard, exposure, vulnerability, and capacity (Cvetković, 2023; Cvetković, 2024a, 2024b; Cvetković & Grbić, 2021; Cvetković, Nikolić, & Ivanov, 2023; Cvetković & Renner, 2024; Cvetković & Šišović, 2024; Cvetković, Tanasić, Renner, Roković, & Beriša, 2024; Cvetković, 2024a; Cvetković, Dragašević, Protić, Janković, Nikolić, & Milošević, 2022). When interpreted through this lens, ransomware can be seen as a digital hazard that can disrupt systems at scale, amplify vulnerabilities, and test institutional readiness to absorb and recover from shocks. Like natural or technological disasters, ransomware strikes often occur abruptly, cause widespread disruption, and require coordinated responses across multiple sectors (Al-ramlawi, El-Mougher, & Al-Agha, 2020; Aleksandrina, Budiarti, Yu, Pasha, & Shaw, 2019; Carla, 2019; Cvetković, 2019; Cvetković & Janković, 2020; Cvetković & Martinović, 2020; Cvetković Šišović, 2024; Cvetković, Tanasić, Ocal, Kešetović, Nikolić, & Dragašević, 2021; Kumiko & Shaw, 2019; Perić & Cvetković, 2019; Vibhas, Bismark, Ruiyi, Anwaar, & Rajib, 2019; Wedawatta, 2012). This perspective broadens the understanding of ransomware—framing it not solely as a cybersecurity issue, but as a form of digital disaster with profound economic, societal, and institutional implications.

Scalability and anonymity uniquely characterise cyberattacks (Tarter, 2017). As digital transformation speeds up, vulnerabilities proliferate across customer channels (Farahbod et al., 2020), impacting business operations, supply chains, and human capital. This occurs unless security is integrated into the initial designs (George et al., 2024). The increasing complexity of cyberspace exacerbates cyber inequalities, widening the gap between large and small businesses and deepening the divide between developed and emerging economies, creating sectoral disparities (World Economic Forum, 2025). Securing a digital future is crucial in this age of technological advancement and interconnectedness. This commitment to effective cybersecurity is essential for individuals, organisations, and societies (Cobos, 2024; Thakur, 2024).

The central aim of this paper is to examine ransomware as a complex, multidimensional threat that extends beyond traditional cybersecurity narratives. These narratives often focus narrowly on technical vulnerabilities, breach response, and system recovery, without addressing large-scale cyber incidents' broader systemic, financial, and social ramifications. By situating ransomware within the broader framework of disaster risk, the study evaluates its immediate financial impacts—such as ransom payments, recovery expenditures, and operational disruption—and its longer-term effects, including reputational harm, institutional instability, and socio-economic disparities. This perspective provides a more holistic understanding of ransomware as a digital hazard with systemic

 doi:10.20944/preprints202504.1950.v1

implications, capable of weakening economic resilience, compromising critical infrastructure, and diminishing public confidence in both governmental and private institutions. Ultimately, the paper seeks to inform the development of integrated risk governance strategies that reflect the dynamic and interconnected nature of today's cyber threat landscape. Methodologically, the study draws upon a structured qualitative framework rooted in multiple case studies. The selected cases span diverse geographical and sectoral contexts and are analysed using thematic coding to identify patterns of financial loss, institutional disruption, and socio-economic consequences.

Also, this study adopts a multiple case study framework, examining sixteen globally significant ransomware incidents between 2015 and 2025. The analysis draws on various sources, including institutional documents, academic publications, and financial reports. The paper is organised as follows: Section 2 reviews the theoretical underpinnings and economic dimensions of cyberattacks; Section 3 introduces a classification of ransomware threats; Section 4 details the research methodology; Sections 5 and 6 analyse the financial, economic, and social impacts; and Section 7 concludes with key takeaways for policy and practical applications.

2. Methods

This research applies a qualitative-descriptive approach, using multiple case studies to explore ransomware's financial, operational, and societal impacts, especially regarding their disaster-like effects and sector-wide ripple impacts. A purposive sampling method selected sixteen significant ransomware cases from 2015 to 2025. These incidents involved private companies, public entities, critical infrastructure, and even national governments. Selection criteria included data availability, financial impact scale, and variation in attack methods and targeted sectors. Data were drawn from various sources: peer-reviewed studies, institutional reports, cybersecurity datasets, published financial records, and media coverage.

A structured thematic analysis was employed to explore the complex impacts of ransomware attacks. The findings were organised into four main categories: (1) direct financial losses, including ransom payments, data recovery costs, and downtime-related expenses; (2) indirect financial losses, such as rising insurance premiums, legal and compliance costs, and revenue decline from lost customers or contracts; (3) broader economic disruptions, encompassing supply chain breakdowns, service delays, productivity losses, and liquidity challenges; and (4) reputational and societal effects, including diminished public trust, psychological strain on employees and citizens, breaches of data privacy, and weakened institutional credibility. This framework offers a holistic view of ransomware—not just as a cybercrime, but as a disruptive phenomenon with disaster-like ramifications across economic and social domains. To frame these findings, the study adopts a disaster risk perspective, treating ransomware as a complex socio-technical threat that can destabilise economies and weaken infrastructure resilience. Cross-case comparisons uncovered recurring patterns and vulnerabilities, forming the basis for policy discussions and governance recommendations in cyber risk management.

3. Impact of Cyber Attacks on Digital Society and Economy

The COVID-19 pandemic has pushed many business entities from the public and mainly private sectors to a hybrid business environment based on remote work. Initially, it positively impacted both the human capital of companies and the economic and financial results. However, it has also caused an exponential increase in risks due to the use of unsecured devices and applications based on Cloud directories for data transfer (Rahman & Islam, 2022), thereby expanding the exposure of companies to potential attacks, while at the same time, cybercriminal actors are taking advantage of this established dependence of individuals and legal entities on digital technologies (Cook et al., 2023).

Table 1. Regional distribution of the cost impact of cyberattacks. Source: Authors calculation based on data (Sviatun, et al., 2021).

 doi:10.20944/preprints202504.1950.v1

Area / Region	Regional GDP (in trill. $)	Costs of cyberattacks (in bill. $)	Losses caused by cyber attacks (in % of GDP)
North America	20.2	140-175	0.69-0.87
Europe & Central Asia	20.3	160-180	0.79-0.89
East Asia and the Pacific	22.5	120-200	0.53-0.89
South Asia	2.9	7-15	0.24-0.52
Latin America and the Caribbean	5.3	15-30	0.28-0.57
Sub-Saharan Africa	1.5	1-3	0.07-0.20
Middle East and North Africa	3.1	2-5	0.06-0.16
Global	75.8	445-608	0.59-0.80

A territorial diversification of the impact of costs and losses from cyber incidents and attacks has been identified, which we see in the results of the authors' empirical research (Sviatun et al., 2021) that the highest loss rate as a percentage of GDP is determined in Europe and Central Asia, North America and East Asia and the Pacific, and countries from these regions are characterised by high income and income rates, more advanced technological infrastructure, a high degree of urbanisation, education, and business digitalisation (Tariq, 2018).

Globally, the impact of cyber attacks on the world economy is significant (Schwarz et al., 2021) because this sophisticated social phenomenon is rooted in deep and comprehensive geographical and socioeconomic causes (Chen et al., 2023). Cyber threats also impact an organisation's revenue, reducing it through lost sales, contracts, market share, additional funding, or licenses. In a business context, these typically include marketing and commercial aspects related to sales. However, we also consider that some revenue may not necessarily have such an origin, for example, in public and non-profit organisations (Couce-Vieira et al., 2020).

A cyber incident that disrupts the functioning of vital service segments of critical infrastructure can cause widespread chaos, endanger lives, and cause long-term socioeconomic damage to the economy. While the security of digital components in critical infrastructure serving essential services is essential to maintaining resilience, the combination of digital capabilities and physical components expands potential new risks arising from the combined effect of digital vulnerabilities and the complexity of the physical world (International Chamber of Commerce, 2024).

4. Vector Modalities and Attack Classification

The digital age has led to a wide range of cybersecurity threats that exploit vulnerabilities in technology, processes, and human behavior (Thakur, 2024). Ransomware, malware, and distributed denial of service (DDoS) are examples of evolving cyberattack methods (Cremer et al., 2022).

Of the above vector modalities, ransomware attacks are classified as a distinct form of high-tech crime experiencing the highest growth rate for years. According to research by Putnik et al. (2022), estimates indicate that every 11 seconds, one legal entity becomes a victim of a ransomware attack. Unlike viruses that attach to trusted files or applications and damage or destroy them when launched, worms are a type of malicious software that spreads without user interaction, causing network congestion, computer system slowdowns, or disruptions in basic operating processes (Thakur, 2024), the evolution of ransomware through improvements in the use of encryption and attack vectors, developed attack monetisation modalities, and financial flows through digital payment currencies, which provide discretion of the identity of the contracting party in repayments, defines it as the prevailing malware today (August, et al., 2019). Since this attack modality is based on extortion, it infects a computer system. Further, it prevents access to files, data, and other confidential information or even access to the entire system.

Initially, they implied human interaction, however, looking at the genesis of development, today it is not necessary for the initial infection and its spread through a computer system, where it is characterised by the characteristics of a worm malware, which moves from the infected to

 doi:10.20944/preprints202504.1950.v1

unprotected systems in the same computer network without interaction and additional participation of the attacker (August, et al., 2022). Today, ransomware, as the fastest growing and most complex type of cyber attack that does not require technical knowledge and has a broad scope of action, while providing anonymity to the attacker, is a serious risk to global economic flows (Chin, 2024).

The relentless evolution of malicious software poses a significant challenge to cybersecurity, with ransomware emerging as a ubiquitous and destructive threat (Krivokapić et al., 2023). Malware, designed to disrupt electronic devices, constantly evolves, hampering efforts to mitigate its impact. The lack of public disclosure regarding malware attacks, driven by concerns about sensitive information and potential reputational damage, hinders collaborative prevention efforts and makes comprehensive research difficult (Muniandy et al., 2024).

Its attack cycle includes exploitation, infection, delivery, execution, backup manipulation, file encryption, user notification, and cleanup (Muniandy et al., 2024). New techniques have increased the profitability of attacks and the likelihood of success. This includes targeting high-value business entities and ransomware as a service (Gulyas & Kiss, 2023), where ransomware criminals sell customised software packages to the user (The Financial Action Task Force, 2023).

Ransomware as a Service (RaaS) refers to a criminal business model in which ransomware criminals provide ransomware software kits on the Dark Web or engage in elements of a ransomware attack, including malware distribution, initial compromise of the victim's network, data exfiltration, or ransom negotiations for affiliates in exchange for a fee and/or a percentage. Criminals may also purchase stolen credentials to access and exploit victim systems that enable ransomware distribution and may obtain intelligence on specific industries in specific jurisdictions to inform their targeting and maximise the effectiveness of their attack (The Financial Action Task Force, 2023). The RaaS model has reduced the cost and technical expertise required to conduct ransomware attacks, lowering the barriers to entry and enabling less sophisticated criminals to conduct ransomware attacks.

As one case study in the research in this paper, ransomware is an economically destructive phenomenon that leads to real-world security consequences that often exceed the costs of paying the ransom. In addition to the loss of revenue that an organisation may suffer, other costs may be obvious, some may not. The more obvious costs include paying the ransom (if paid); remediation of the incident, new hardware, software, and incident response services; insurance deductibles; legal fees and litigation; and public relations (Seng et al., 2024).

Financially motivated ransomware attacks utilise vectors such as email, spam, and phishing, making tracking difficult due to using virtual currencies such as Bitcoin to pay ransoms. Several notable ransomware variants, including: BadRabbit, BitPaymer, Cerber, Cryptolocker, Dharma, DoppelPaymer, GandCrab, Locky, Maze, MeduzaLocker, NetWalker, NotPetya, Petya, REvil, Ryuk, SamSam, and WannaCry, have contributed to this evolving threat landscape (Muniandy et al., 2024), some of which are sampled for analysis in this study.

5. Classification of Ransomware Costs and Expenses

A comprehensive approach to the economic aspects of cybersecurity must include a thorough consideration of the direct and indirect costs of cybersecurity measures, as pointed out by researchers (Lis & Mendel, 2019), and the expected damage caused by cyberattacks, especially the type of ransomware attacks studied in the cyberspace of the digital economy. Financial motives for cyber incidents and attacks are the dominant motive in their analysis, accounting for 74% of detected cyber incidents globally and 80% in high-income countries, according to Cobos (2024). In contrast, only 41% of detected incidents in developing countries were primarily financially driven.

By differentiating costs in accounting, a clear division has been formed into direct and indirect costs arising from a cyber attack (Cashell et al., 2004). In this case, direct costs include returning the entire computer system to its original state before the cyber incident, which include additional expenditures on labor and materials but also depend on increased resource expenditures on cybersecurity (software or hardware upgrades).

 doi:10.20944/preprints202504.1950.v1

Direct cost is the monetary equivalent of losses, damage, or other suffering experienced by an individual victim as a result of a cyber attack, which includes loss of monetary value and related inconvenience (Wang et al., 2019). When accounting and financial treatment of investment costs in cybersecurity, it is necessary to consider, according to Kunzler (2023), the investment matrix between the potential costs of a cyber attack, its risks and the costs of security measures. Then there are the costs arising from the interruption of the entity's operational business, which include lost revenue from the sale of goods, works and services, as well as the loss of productivity, which, under the influence of the domino factor, spreads to customers (Fotis, 2024) but also suppliers (Jimmy, 2024), as well as to the entire organisation (Onuka et al., 2023).

Indirect costs include the type of costs that tend to increase after a cyberattack and immediately after the initial damage to the business entity is repaired, and arise from loss of reputation, damage to the brand, loss of customers, insurance costs and premiums (ThankGod, 2024), litigation and tax costs, economic damage to the parent entity's subsidiaries, higher investments in cybersecurity for preventive response and opportunity costs of budget resource allocation. They are mainly associated with the economic concept of negative externalities on third parties (Lis & Mendel, 2019). Therefore, indirect costs are characterised by a predominantly intangible nature (Wang et al., 2019), and their consequences are multiple because they affect different aspects of the business, consumers and the broader economy (Cobos et al., 2024).

Table 2. Typology of the most significant direct and indirect losses and costs caused by ransomware attacks.

Direct losses	Indirect losses
Payment of the ransom	Recovery process which includes investigation costs, verification costs for checking the system (diagnostics and remediation) and restoration costs to restory the system to the network (testing)
Data breach	Loss of data as an operating loss caused by business interruption
Other claims for liability for losses suffered by third parties	Loss of customers and business clients
The market value or replacement value of the property or servicies destroyed	Loss of reputation

The critical distinction between the direct and indirect costs of ransomware attacks lies in the exponential growth potential of indirect losses arising from them, compared to the finite limit of direct losses. This dynamic represents a disproportionate burden on society (Cobos, 2024) and has far-reaching consequences for the digital economy, which spills over into the real physical economic sector and business.

6. Analysis and Financial Assessment of the Consequences

The analysis shows that cybersecurity is a multidimensional, heterogeneous and dynamic challenge among countries that may face different optimization problems depending on their threat environment (Cobos, 2024) and that encompasses economic, political, social, digital and technical-technological aspects. The distribution and proliferation of detected cyber incidents by income and geographical regions is complex and influenced by several interrelated factors such as economic prosperity, political stability, cybersecurity capacity and geopolitical tensions (Cobos et al., 2024).

Investing in security technologies represents a capital expenditure. However, as Lee (2021) states, the optimal investment comes at the point where the marginal increase in the price of a cyber investment is equal to the marginal reduction in the financial loss from a cyber attack. Analyzing the subject sample through case studies, it was found that the implementation of robust cybersecurity measures effectively reduced the occurrence of financial data breaches, and that through

 doi:10.20944/preprints202504.1950.v1

comprehensive encryption protocols and multi-factor authentication, organizations were able to improve the security of sensitive financial information (Grace, 2023).

Based on available data, the median reported direct loss and damage to a company from all cyber incidents was around $0.4 million, with three-quarters of reported losses below $2.8 million (International Monetary Fund, 2024). However, The distribution is highly skewed, with some incidents imposing losses in the hundreds of millions of US dollars and even accumulating financial damage of several billion dollars. Such extreme losses can lead to liquidity problems for business entities and even threaten their solvency.

Ransomware can cause significant negative consequences for the victim, including non-recovery and recoverable costs. The various types of damages that can occur include financial losses, including ransom payments and the recovery process, operational loss caused by business interruption, and data loss caused by data breaches, which will be discussed in detail below. However, ransomware can also affect third parties, giving rise to liability claims for losses suffered by third parties, loss of customers, and reputational damage (Krivokapić et al., 2023).

Econometric analysis suggests that digitalization and geopolitical tensions significantly increase the risk of cyber incidents (International Monetary Fund, 2024). Based on an extensive survey of available data from previous empirical research, literature, news articles, and official databases of international institutions reporting on cyber attacks, the analysis identified the factors of financial damage, expenditures, and costs caused by ransomware attacks in a sample of 16 case studies over the period 2015 to 2025.

Table 3 outlines the direct and indirect financial damages linked to sixteen major ransomware incidents reported between 2015 and 2025. Direct losses range from moderate figures—such as $1.87 million in the Technion University case—to extreme levels, including the $10 billion damages reported in the MOVEit and NotPetya attacks. While direct costs are often substantial, indirect losses carry even more profound implications. These include legal fees, regulatory fines, system recovery expenses, and long-term disruptions to business continuity. Particularly severe financial impacts were observed in critical infrastructure and healthcare systems cases. Overall, the findings underscore the disproportionate growth of indirect costs relative to direct ones, highlighting ransomware's potential to trigger systemic economic instability.

Table 3. Analysis of financial damage, expences and costs of ransomware attacks in period 2015-2025 business year. Source: authors calculation and research.

No.		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Case study		**Cryptolocker (2015)**	**SamSam Ransomware (2016-2018)**	**Locky Ransomware (2016-2018)**	**Malicious program code "NotPetya" (2017)**	**Ransomware attack „WannaCry" (2017)**	**Ryuk Ransomware (2018–present)**	**DoppelPayment Ransomware (2019-present)**	**Company "Enel Group" (2020)**
Financial damage, expences and costs	**Direct**	$18 million	$6 million	$1 billion	$10 billion	$4 billion	$150 million	$43,27 million	$14 million
	Indirect	Costs for remediation of damage to computer systems and restoration of operational processes, loss of production, loss of reputation	$30 million	Costs caused by the loss of important data, significant disruptions in the functioning of organisations. Loss of productivity where business entities were forced to invest large amounts in	Losses due to production disruptions, delivery delays, and additional costs for recovery and investments in cybersecurity	Millions of dollars in losses due to impact on key services and organisations	Loss of data, downtime, loss of reputation	Loss of data, reputational damage, disrupted operation of organisations	$84.02 million (data recovery expenses, legal fees, and disclosure fees - company GDPR compliance penalties)

 doi:10.20944/preprints202504.1950.v1

			the recovery of the system, which led to exponential growth in operating expenses					
No.		**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Case study		**Company "Garmin" (2020)**	**Company „Kaseya Inc.“ (2021)**	**Company „Colonial Pipeline“ (2021)**	**Republic of Costa Rica (2022)**	**Data Transfer Software "MOVEit" (2023)**	**University and Research Institute "Technion" (2023)**	**Company „Change Healthcare Inc.“ (2024)**	**Company "Southern Water" (2025)**
Financial damage, expences and costs	**Direct**	$10 million	$70 million	$4,4 million	$1.66 billion (2.4% of the country's GDP)	$10 billion	$1.87 million (80 bitcoin - BTC)	$22 million	$5,7 million
	Indirect	$15.2 million in damages and further costs of service interruptions, loss of revenue from disabled apps and services, legal costs, class action lawsuit	Loss of revenue due to service interruptions, legal costs and capital expenditures for system restoration	Estimated losses of over $420 million per day.Costs due to downtime in operations: loss of revenue, breach of contractual obligations, increased operating costs due to system restoration and crisis management.	Increased costs for repairs and restoration of the system. Negative impact on import/export logistics.	Multiplier factor of ongoing costs (operating costs due to business downtime, legal costs and damages to affected users)	Postponement of exams, blocking networks, temporary loss of access to data, blocking of the website. Loss of reputation and trust in academic institutions.	$8.87 billion ($2.87 billion - response costs and $6 billion - assistance to health care providers, as well as litigation costs)	Costs for system recovery, loss of confidence in security, increased costs on technological improvements

Table 4 broadens the focus by categorising each incident's economic and social outcomes. A consistent pattern emerges: essential services—healthcare, transportation, education, and public administration—are frequently disrupted. These service interruptions are often accompanied by public distrust, reputational setbacks, and heightened psychological stress. In critical cases like WannaCry and Colonial Pipeline, the consequences escalated into public safety concerns, prompting governmental intervention and emergency actions. This division between economic and social impacts further illustrates the multifaceted nature of ransomware, resembling disaster events in their capacity to disrupt digital infrastructures and societal stability.

Table 4. Analysis of economic and social consequences of ransomware attacks in period 2015-2025 business year. Source: Authors calculation and research.

No.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Case study	**Cryptolocker (2015)**	**SamSam Ransomware (2016-2018)**	**Locky Ransomware (2016-2018)**	**Malicious program code "NotPetya" (2017)**	**Ransomware attack „WannaCry“ (2017)**	**Ryuk Ransomware (2018–present)**	**DoppelPaymer Ransomware (2019-present)**	**Company "Enel Group" (2020)**

 doi:10.20944/preprints202504.1950.v1

Consequences	Economic	Huge drop in production, interruption in operations, long-term consequences on business productivity	Significant disruptions in work processes, increased recovery costs, loss of efficiency	Increased recovery costs, loss of trust in IT security, large technological investments for recovery	Big losses in global companies such as Maersk, FedEx, Merck and others. Disruption in the transport and logistics sector. Increase in the price of goods that did not arrive on time.	The enormous damage to large corporations, especially in industries such as healthcare and logistics, has an economic impact on a global scale.	Major business interruptions, disruption of public services (especially in health care and municipalities)	Significant recovery costs, loss of trust in IT security, high costs of legal and security services	Huge financial costs on restoring the system and recovering from attacks
	Social	Loss of personal data, stress for individuals, erosion of trust in data security	Deterioration of public confidence in the safety of infrastructure, stress for citizens	Erosion of user and patient trust, stress for employees, data privacy risks	Increased distrust in public and private financial institutions, a decrease in spending, and an impact on confidence in the health sector as vaccine production was interrupted.	Disruptions to public services, especially in health care facilities, cancellations of 19,000 medical appointments, loss of life in some cases, negative impact on the business of NHS, FedEx, Telefónica, and others	Deterioration of public trust in data and infrastructure security, stress for workers and citizens	Potential loss of life (in the case of the Düsseldorf hospital), violation of public trust, stress for employees	Potential loss of customer trust, impact on reputation and data security

No.	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Case study	**Company "Garmin" (2020)**	**Company „Kaseya Inc.“ (2021)**	**Company „Colonial Pipeline“ (2021)**	**Republic of Costa Rica (2022)**	**Data Transfer Software "MOVEit" (2023)**	**University and Research Institute "Technion" (2023)**	**Company „Change Healthcare Inc.“ (2024)**	**Company "Southern Water" (2025)**
Consequences **Economic**	Increased risk of future attacks, reputational damage, system restoration costs, and legal costs	Disruption of many companies, increased renewal costs, legal processes, decline in trust in the IT sector	Fuel outages were reported across the U.S. Southeast, especially in states such as Georgia, North Carolina, and Virginia. People panicked and bought fuel, which led to shortages at supply stations.	Disruptions in fiscal and tax systems, non-payment of salaries to employees, paralysis of public services.	Global revenue losses for affected firms and organisations, loss of competition in specific sectors	Disruptions to the work of the university, postponement of important academic activities, such as exams, affecting students and the academic calendar. Potential risk to research and sensitive data in the field of cybersecurity.	Severe disruptions in the processing of medical claims and payments, significant disruptions in the healthcare industry	Loss of data, interruption in water supply, damage to reputation

 doi:10.20944/preprints202504.1950.v1

Social	Loss of customer trust, possible negative impact on corporate reputation and future sales	Difficulties for small and large companies, reducing trust in the security of digital platforms	Gas stations have been closed, fuel prices have risen, and transportation has been disrupted, including air travel. Citizens and public services have felt the effects of fuel shortages. Social tensions due to shortages.	There is a growing concern among citizens about disrupted government services and an increased fear of compromised sensitive data. The impact on the public sector and the living standards of citizens who depend on state services, as well as the increased burden on public services.	65 million users harmed, privacy violations, personal and corporate data compromised	Loss of confidence in the security of academic institutions, disruptions in student activities. Public pressure on the university and the government to respond to the attacks.	Data exposure of 190 million people, massive legal proceedings, patient trust significantly damaged	Potential disruption of services for citizens, increased stress for employees

Table 5 details the attack vectors and techniques used across the analyzed cases, revealing a clear progression in complexity. Early methods, such as phishing emails and malware attachments (e.g., CryptoLocker, Locky), have evolved into advanced, multi-vector attacks employing zero-day exploits, supply chain breaches, and ransomware-as-a-service models. Tactics now often include automation, stolen credentials, and lateral movement within networks, reflecting a trend toward scalable, professionalized cybercrime. Encrypted communications and anonymous payment systems—most notably cryptocurrency wallets—continue to hinder attribution and response. This evolution supports the interpretation of ransomware as more than just a criminal act, positioning it as a form of digital disaster within contemporary risk governance frameworks.

Table 5. Analysis of vector metodology of ransomware attacks in period 2015-2025 business year. Source: Authors calculation and research.

No.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Case study	**Cryptolocker (2015)**	**SamSam Ransomware (2016-2018)**	**Locky Ransomware (2016-2018)**	**Malicious program code "NotPetya" (2017)**	**Ransomware attack „WannaCry“ (2017)**	**Ryuk Ransomware (2018–present)**	**DoppelPayment Ransomware (2019-present)**	**Company "Enel Group" (2020)**
Vector methodology of cyber attack and incident	Phishing emails, malicious attachments, data encryption, and ransom demand	Manual delivery, attacks on JBoss servers, abuse of RDP and VPN vulnerabilities, privilege escalation, subsequent data encryption	Phishing attacks use malicious Word documents to trigger macros, leading to ransomware downloads. Once activated, Locky encrypts a large number of different types of	An attack through compromised Legitimate Software Updates (M.E.Doc). The malware spread like a worm, disguised as ransomware, but the goal was to cause destruction, not extort money.	The attack exploited a security vulnerability in Microsoft Windows operating systems (EternalBlue exploit)	An attack that begins with a compromise of a network (usually a TrickBot), delivered manually, with network mapping and data exfiltration before launching an attack.	Sfir -phishing attacks, exploitation of out-of-date vulnerabilities, network mapping, privilege escalation, fast encryption of offline data	Attack via Netwalker and Snake ransomware, encrypting data within the company

 doi:10.20944/preprints202504.1950.v1

			data, including data on network parts. It used a combination of RSA and AES encryption, which made the data inaccessible without a decryption key that could only be obtained after paying the ransom.					
No.	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Case study	**Company "Garmin" (2020)**	**Company „Kaseya Inc.“ (2021)**	**Company „Colonial Pipeline“ (2021)**	**Republic of Costa Rica (2022)**	**Data Transfer Software "MOVEit" (2023)**	**University and Research Institute "Technion" (2023)**	**Company „Change Healthcare Inc.“ (2024)**	**Company "Southern Water" (2025)**
Vector methodology of cyber attack and incident	The attack used WastedLocker, which was developed by the notorious group Evil Corp. Systems were encrypted, and services such as Garmin Connect, flyGarmin, Strava, and inReach were disabled. The attackers demanded $10 million to decrypt the data.	The attack was carried out through Kaseya V.S.A. software, which allowed malware to be inserted, encrypting data on more than 1,000 systems. The attackers demanded a ransom of $70 million in Bitcoin.	The attackers, who were members of the hacker group Darkside, gained access through an employee's VPN account and applied data encryption software.	The attackers used ransomware to coordinate attacks on multiple government agencies (Ministry of Finance, Ministry of Education, Social Security Fund).	Ransomware group "Clop" exploited a zero vulnerability in "MOVEit" software	The attackers used the software DarkBit, which targets Windows operating systems. They added the "Darkbit" to the "AES-256" encryption to encrypt data.	Citrix portal without multi-factor authentication, data exfiltration, file encryption	Attack through Black Basta ransomware, use of phishing attacks or vulnerabilities in the network

7. Discussion

The evidence presented in this paper reinforces the classification of ransomware as a high-impact, cross-border threat that mirrors large-scale disruptive events typically categorized as disasters. Its spread through digital infrastructure, exploitation of systemic weaknesses, and far-reaching secondary effects—particularly on public trust, service continuity, and social stability—position ransomware within the broader category of complex socio-technical risks requiring coordinated, multisectoral responses (Andersen, 2025; Axon et al., 2023; Connolly & Wall, 2019; Moussaileb, Cuppens-Boulahia, Lanet, & Bouder, 2021; Nagar, 2024; Robles-Carrillo & García-Teodoro, 2022; Singh & Sittig, 2016; Sudheer, 2024; Wilner et al., 2019; Yuste & Pastrana, 2021).

Notably, the concentration of indirect and intangible costs in essential sectors like healthcare, utilities, and government services reveals a significant policy gap: the absence of adaptive cyber

 doi:10.20944/preprints202504.1950.v1

resilience frameworks tailored to critical infrastructure (Cvetković, 2013; Cvetković & Kezunović, 2021; Cvetković, 2024b; Hromada & Lukas, 2012; Koliou, van de Lindt, Ellingwood, Dillard, Cutler, & McAllister, 2018; Mijalković & Cvetković, 2013; Vidović, Cvetković, & Beriša, 2024). This issue is especially pressing in transition and lower-capacity economies, where digital advancement often outpaces the development of effective risk management systems. The proliferation of ransomware-as-a-service (RaaS) further enlarges the threat landscape, increasing the volume of attacks and diversifying their targets—strengthening the case for framing ransomware as an evolving disaster phenomenon.

In the last ten years, an exponential growth of ransomware strains and changes in the malware market have been identified, which implicitly affect the challenges, risks, and threats to the barrier that prevents large-scale cyber attacks (August et al., 2019). A comprehensive analysis of empirical evidence and data has produced a systematic overview in Tables 3, 4 and 5 of this paper. The period from 2015 to 2019 was identified in the analysis as an early period of gradual but exponential growth in cybercrime, including ransomware attacks, which accumulated significant losses and financial damage, primarily direct and indirect costs determined to be unpredictable per attack. The most significant case studies were found to be the "Locky", "NotPetya" malware and "WannaCry" ransomware attacks. Then, from the end of 2019, the crisis caused by the coronavirus pandemic occurred, which in 2020 was a catalyst for the development and vector distribution of ransomware attacks through a rapid degree of digitalisation and the establishment of a hybrid business model, primarily on critical infrastructure as a vital interest of every state, through the health sector, the financial sector and the energy sector.

Collectively, the findings from Tables 3, 4, and 5 strengthen the framing of ransomware as a form of digital disaster. These incidents share key characteristics with traditional disasters—unpredictability, large-scale disruption, cascading impacts, and significant financial and human costs. The comparative analysis highlights that attacks targeting healthcare and government sectors often result in the highest indirect losses and the most profound societal consequences. This underscores the need for cyber resilience efforts to prioritize sectors that are both highly dependent upon and vulnerable to digital infrastructure. Additionally, the evolution of attack methods indicates the necessity for ongoing adaptation in technical defenses and organizational risk management strategies.

By establishing continuous monitoring of threats arising from ransomware attacks, it was found that in 2021 there were record ransom payments for ransomware attacks ($ 1.1 billion), which indicated the growth of cybercrime and the characteristic of greater profitability of cyberspace attacks on the digital economy. In 2022, the number of reported cyberattacks continued to grow, and the financial damages were significant - indicating increased incidents and a growing, primarily negative impact on the economy. Total global losses from cyberattacks in 2023 exceeded $12.5 billion, an increase of 22% compared to the previous year. Ransomware attacks were among the most significant. In the first half of 2024, payments from victims of ransomware attacks reached $460 million, an increase of 2% compared to the same period in 2023. Projections indicate a continued growth trend in cyberspace attacks, of which ransomware attacks are the type with the most significant impact on the digital economy, with devastating socio-economic consequences for the economy and population, and above all for critical infrastructure.

From a governance standpoint, these findings underscore the urgent need for integrated risk management strategies that extend beyond technical enhancements. Governments should incorporate cyber-disaster scenarios into national emergency planning, mandate cyber incident reporting, and incentivize investments in cyber hygiene—particularly within the public sector. The response must go beyond infrastructure security for private-sector organizations, especially in finance, health, and energy. It should also strengthen organizational resilience through staff training, redundancy protocols, robust data recovery planning, and insurance coverage reflecting contemporary digital risks. Public-private partnerships and shared platforms for threat intelligence are key to managing sectoral interdependencies.

 doi:10.20944/preprints202504.1950.v1

At the international level, the extraterritorial nature of ransomware calls for deeper collaboration on attribution, enforcement, cryptocurrency oversight, and intelligence exchange. Finally, future research should prioritize the development of quantitative models that capture both direct and cascading costs, as well as scenario-based simulations to assess sector-specific preparedness. Longitudinal studies tracking recovery trajectories post-attack could further enrich the understanding of institutional resilience, complementing the cross-sectional insights provided in this study.

8. Conclusions

This paper has shown that ransomware should no longer be viewed solely as a cybersecurity challenge, but as a complex and evolving disaster risk with far-reaching consequences for economic stability, institutional resilience, and public trust. Drawing on sixteen high-impact case studies, the research offers a typology of financial losses and systemic disruptions, emphasizing the disproportionate effects on critical infrastructure and the compounding nature of indirect costs. By framing ransomware as a form of digital disaster, the study contributes to a more integrated approach to cyber risk within the broader context of disaster risk governance and resilience planning.

The findings point to several practical implications, calling for coordinated but context-specific action from key stakeholders: a) governments should incorporate ransomware preparedness into national risk strategies, encourage transparent incident reporting, and provide fiscal incentives for cybersecurity investments; b) private-sector entities need to implement zero-trust architectures, develop insurance solutions tailored to cyber threats, and enhance organisational resilience that extends beyond technical safeguards; c) at the international level, institutions must advance cross-border collaboration—particularly in regulating virtual assets, supporting joint law enforcement efforts, and setting global standards for cyber disaster response.

The financial impact of cybercrime has reached staggering proportions, with projections indicating an alarming upward trend. An unfortunate aspect of today's online society affects businesses of all sizes. The global scale of financial flows associated with ransomware attacks has grown dramatically in recent years. New techniques have increased the profitability of attacks and the likelihood of success. These include targeting large, high-value entities and ransomware-as-a-service, where ransomware criminals sell customized software kits to affiliates. The consequences of a ransomware attack can be dire and pose national security threats, including damage and disruption to critical infrastructure and services. A ransomware attack is a form of extortion and FATF standards require it to be criminalized as a predicate offense for money laundering (The Financial Action Task Force, 2023). Ransomware criminals exploit the international nature of virtual assets to facilitate large, near-instantaneous cross-border transactions, sometimes without the involvement of traditional financial institutions that have programs in place to prevent money laundering and terrorist financing.

Ransomware attacks are on the rise globally, and any business or organization can be a target of these attacks, which requires additional attention and preparation in terms of business cyber security and the complete protection of the digital economy. As Krivokapić et al. (2023) point out, it is crucial that all relevant institutions, including financial institutions, are informed about the ransomware attack and the ransom payment. This is important because it provides sufficient evidence for possible legal proceedings or cancellation of ransom payments. Also, business entities should invest in insurance policies that include cybersecurity, as general commercial policies do not provide sufficient protection against cyber attacks. These insurances help cover the costs arising from attacks such as ransomware (Cobos et al., 2024). Since states cannot always effectively protect themselves from cyber attacks, it is recommended that they encourage investment in cybersecurity. This can be supported by introducing tax breaks and double deductions for costs related to cybersecurity.

The first recommendation is to continue investing in workforce education and training, so that individuals can identify threats and respond effectively (World Economic Forum, 2025). Then, it is necessary to adopt a zero-trust approach, which minimizes the risk of attacks by treating all requests

 doi:10.20944/preprints202504.1950.v1

as potentially malicious. It is also important to improve incident response plans to respond quickly to cyberattacks and reduce their impact. Advanced technologies, such as artificial intelligence and automation, should be used to improve threat detection and predictive analytics, but with caution against attacks launched by artificial intelligence (Thakur, 2024). Collaboration and information sharing between members of the cybersecurity community is also key to strengthening defenses. Data protection and privacy should be a priority, along with regulatory compliance and transparent communication. Finally, it is important to regularly assess and update security to identify new vulnerabilities and adapt defenses to new threats, because cybersecurity is an ongoing process, requiring a proactive approach, collaboration, and integration of modern technologies to successfully confront evolving threats.

This study has limitations. The analysis relies on publicly available data, which may exclude undisclosed or underreported incidents. Future research should focus on longitudinal data, sector-specific vulnerabilities, and modeling recovery trajectories after major ransomware events. In closing, confronting the ransomware threat demands more than just technological fixes. It requires a fundamental shift in how digital risk is conceptualised, governed, and financed. Without integrated, adaptive, and inclusive strategies, ransomware may become one of this century's defining disaster threats.

Funding: This research was funded by the Scientific–Professional Society for Disaster Risk Management, Belgrade (https://upravljanje-rizicima.com/, accessed on 18 April 2025) and the International Institute for Disaster Research (https://idr.edu.rs/, accessed on 18 April 2025), Belgrade, Serbia.

Acknowledgements: The authors acknowledge the use of Grammarly Premium and ChatGPT 4.0 in the process of translating and improving the clarity and quality of the English language in this manuscript. The AI tools assisted in language enhancement but were not involved in developing the scientific content. The authors take full responsibility for the manuscript's originality, validity, and integrity.
Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Aleksandrina, M., Budiarti, D., Yu, Z., Pasha, F., & Shaw, R. (2019). Governmental Incentivization for SMEs' Engagement in Disaster Resilience in Southeast Asia. *International Journal of Disaster Risk Management, 1*(1), 32-50.
2. Al-ramlawi, A., El-Mougher, M., & Al-Agha, M. (2020). The Role of Al-Shifa Medical Complex Administration in Evacuation & Sheltering Planning. *International Journal of Disaster Risk Management, 2*(2).
3. Andersen, E. S. (2025). How to mitigate ransomware risk through data and risk quantification. *Cyber Security: A Peer-Reviewed Journal*. doi:10.69554/ztgt3456
4. August, T., Dao, D., & Niculescu, M. F. (2019). Economics of ransomware attacks. Unpublished manuscript.
5. August, T., Dao, D., & Niculescu, M. F. (2022). Economics of ransomware: Risk interdependence and large-scale attacks. Management Science, 68(12), 8979–9002. https://doi.org/10.1287/mnsc.2021.4216
6. Axon, L., Erola, A., Agrafiotis, I., Uuganbayar, G., Goldsmith, M., & Creese, S. (2023). Ransomware as a Predator: Modelling the Systemic Risk to Prey. *Digital Threats: Research and Practice, 4*, 1-38. doi:10.1145/3579648
7. Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*. doi:10.1016/j.iotcps.2023.12.001
8. Carla S, R. G. (2019). School-community collaboration: disaster preparedness towards building resilient communities. *International Journal of Disaster Risk Management, 1*(2), 45-59.
9. Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks (CRS RL32331). Congressional Research Service.
10. Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. Humanities and Social Sciences Communications, 10, 71. doi:10.1057/s41599-023-01560-x

 doi:10.20944/preprints202504.1950.v1

11. Chin, K. (2024). The impact of cybercrime on the economy. Retrieved from https://www.upguard.com/blog/the-impact-of-cybercrime-on-the-economy
12. Cobos, E. V. (2024). Cybersecurity economics for emerging markets. Washington, DC: World Bank. doi:10.1596/978-1-4648-2120-2
13. Cobos, V., Belen, E., & Selcen, C. (2024). A review of the economic costs of cyber incidents. Washington, DC: World Bank Group. Retrieved from http://documents.worldbank.org
14. Connolly, L., & Wall, D. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Comput. Secur., 87*. doi:10.1016/J.COSE.2019.101568
15. Connolly, L., Wall, D., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *J. Cybersecur., 6*. doi:10.1093/cybsec/tyaa023
16. Cook, S., Giommoni, L., Trajtenberg Pareja, N., Levi, M., & Williams, M. L. (2023). Fear of economic cybercrime across Europe: A multilevel application of routine activity theory. The British Journal of Criminology, 63(2), 384–406. doi:10.1093/bjc/azac093
17. Couce-Vieira, A., Insua, D. R., & Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. Decision Analysis, 17(4), 356–374. doi:10.1287/deca.2020.0421
18. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3), 698–722. doi:10.1057/s41288-021-00233-9
19. Cvetković, S. M., & V. (2013). *Vulnerability of critical infrastructure by natural disasters.* Paper presented at the National critical infrastructure protection, regional perspective., Belgrade.
20. Cvetković, V. (2019). Risk Perception of Building Fires in Belgrade. *International Journal of Disaster Risk Management, 1*(1), 81-91.
21. Cvetković, V. (2023). A Predictive Model of Community Disaster Resilience based on Social Identity Influences (MODERSI). *International Journal of Disaster Risk Management, 5*(2), 57-80.
22. Cvetković, V. (2024a). Disaster Risk Management. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.
23. Cvetković, V. (2024b). Essential Tactics for Disaster Protection and Rescue. *Scientific-Professional Society for Disaster Risk Management, Belgrade*.
24. Cvetković, V. M. (2024a). Disaster Resilience: Guide for Prevention, Response and Recovery. In: Belgrade: Scientific-Professional Society for Disaster Risk Management.
25. Cvetković, V. M. (2024b). In-Depth Analysis of Disaster (Risk) Management System in Serbia: A Critical Examination of Systemic Strengths and Weaknesses.
26. Cvetković, V. M., & Šišović, V. (2024). Capacity building in Serbia for disaster and climate risk education. In *Disaster and Climate Risk Education: Insights from Knowledge to Action* (pp. 299-323): Springer Nature Singapore Singapore.
27. Cvetković, V. M., Dragašević, A., Protić, D., Janković, B., Nikolić, N., & Milošević, P. (2022). Fire safety behavior model for residential buildings: Implications for disaster risk reduction. *International Journal of Disaster Risk Reduction, 76*, 102981. doi:https://doi.org/10.1016/j.ijdrr.2022.102981
28. Cvetković, V. M., Renner, R., & Jakovljević, V. (2024). Industrial Disasters and Hazards: From Causes to Conse-quences—A Holistic Approach to Resilience. *International Journal of Disaster Risk Management, 6*(2), 149-168.
29. Cvetković, V. M., Tanasić, J., Ocal, A., Kešetović, Ž., Nikolić, N., & Dragašević, A. (2021). Capacity Development of Local Self-Governments for Disaster Risk Management. *International Journal of Environmental Research and Public Health, 18*(19), 10406.
30. Cvetković, V., & Grbić, L. (2021). Public perception of climate change and its impact on natural disasters. *Journal of the Geographical Institute Jovan Cvijic*.
31. Cvetković, V., & Janković, B. (2020). Private security preparedness for disasters caused by natural and anthropogenic hazards. *International Journal of Disaster Risk Management, 2*(1), 23-33.

 doi:10.20944/preprints202504.1950.v1

32. Cvetković, V., & Kezunović, A. (2021). Security Aspects of Critical Infrastructure Protection in Anthropogenic Disasters: A Case Study of Belgrade. *Research Squares - Preprint*, 10.21203/rs.21203.rs-927528/v927521.
33. Cvetković, V., & Martinović, J. (2020). Inovative solutions for flood risk management. *International Journal of Disaster Risk Management, 2*(2), 71–100.
34. Cvetković, V., & Renner, R. (2024). Comprehensive Databases on Natural and Man-Made (Technological) Hazards and Disasters: Mapping Risks and Challenges. In: Belgrade: Scientific-Professional Society for Disaster Risk Management.
35. Cvetković, V., & Šišović, V. (2024). Understanding the Sustainable Development of Community (Social) Disaster Resilience in Serbia: Demographic and Socio-Economic Impacts. Sustainability, 16 (7), 2620. In.
36. Cvetković, V., Nikolić, A., & Ivanov, A. (2023). The Role of Social Media in the Process of Informing the Public About Disaster Risks. *Journal of Liberty and International Affairs, 9*(2), 104-119.
37. Cvetković, V., Tanasić, J., Renner, R., Roković, V., & Beriša, H. (2024). *Comprehensive Risk Analysis of Emergency Medical Response Systems in Serbian Healthcare: Assessing Systemic Vulnerabilities in Disaster Preparedness and Response.* Paper presented at the Healthcare.
38. Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. Journal of Business and Behavioral Sciences, 32(1), 63–71.
39. 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. doi:10.5281/zenodo.10639463
40. Goodell, J., & Corbet, S. (2022). Commodity market exposure to energy-firm distress: Evidence from the Colonial Pipeline ransomware attack. *Finance Research Letters*. doi:10.1016/j.frl.2022.103329
41. Grace, J. (2023). Impact of cybersecurity measures on financial data breaches. International Journal of Modern Risk Management, 1(1). Retrieved from https://www.iprjb.org/journals/index.php/IJMRM/article/view/2097
42. Gulyas, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. Procedia Computer Science, 219, 84–90.
43. HISCOX Group. (2024). Cyber readiness report 2024: Protecting reputation through cyber resilience. Retrieved from https://www.hiscoxgroup.com/sites/group/files/documents/2024-10/HSX245–2024-CRR.pdf
44. Hromada, M., & Lukas, L. (2012). Critical Infrastructure Protection and the Evaluation Process. *International Journal of Disaster Recovery and Business Continuity, 3*.
45. International Chamber of Commerce. (2024). Protecting the cybersecurity of critical infrastructure and their supply chains.
46. International Monetary Fund. (2024). Global financial stability report: The last mile – Financial vulnerabilities and risks.
47. Jimmy, F. (2024). Assessing the effects of cyber attacks on financial markets. Journal of Artificial Intelligence General Science, 6(1), 288–305. doi:10.60087/jaigs.v6i1.254
48. Jurišić, D., & Marceta, Z. (2024). Collaborative Gaps: Investigating the Role of Civilian-Religious Authority Disconnection in Psychosocial Support Provision during the 2014 Floods. *International Journal of Disaster Risk Management, 6*(2), 1-18.
49. Kala, E. S. M. (2023). Critical role of cyber security in global economy. Open Journal of Safety Science and Technology, 13(4), 231–248.
50. Koliou, M., van de Lindt, J. W., Ellingwood, B., Dillard, M., Cutler, H., & McAllister, T. P. (2018). A critical appraisal of community resilience studies: Progress and challenges.
51. Krivokapić, Đ., Nikolić, A., Stefanović, A., & Milosavljević, M. (2023). Financial, accounting and tax implications of ransomware attack. Studia Iuridica Lublinensia, 32(1), 191–211. Retrieved from https://ssrn.com/abstract=4562912
52. Kumiko, F., & Shaw, R. (2019). Preparing International Joint Project: Use of Japanese Flood Hazard Map in Bangladesh. *International Journal of Disaster Risk Management, 1*(1), 62-80.

 doi:10.20944/preprints202504.1950.v1

53. Künzler, F. (2023). Real cyber value at risk: An approach to estimate economic impacts of cyberattacks on businesses (Master's thesis). University of Zurich.
54. 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.
55. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies, 17(2), 220–239. doi:10.14254/2071-8330.2024/17-2/12
56. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659–671. doi:10.1016/j.bushor.2021.02.022
57. Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. Economics and Business Review, 19(2), 24–47. doi:10.18559/ebr.2019.2.2
58. Mijalković, S., & Cvetković, V. (2013). *Vulnerability of critical infrastructure by natural disasters.* Paper presented at the National critical infrastructure protection, regional perspective.
59. Mokhele, M. O. (2024). Centres or Units: Making Sense of Decentralisation of Disaster Management in South African Municipalities. *International Journal of Disaster Risk Management, 6*(2), 19-38.
60. Molina, R. M. A., Torabi, S., Sarieddine, K., Bou-Harb, E., Bouguila, N., & Assi, C. (2022). On Ransomware Family Attribution Using Pre-Attack Paranoia Activities. *IEEE Transactions on Network and Service Management, 19*, 19-36. doi:10.1109/tnsm.2021.3112056
61. Molnár, A. (2024). A Systematic Collaboration of Volunteer and Professional Fire Units in Hungary. *International Journal of Disaster Risk Management, 6*(1), 1-13.
62. Mott, G., Turner, S., Nurse, J., Pattnaik, N., MacColl, J., Huesch, P., & Sullivan, J. (2024). 'There was a bit of PTSD every time I walked through the office door': Ransomware harms and the factors that influence the victim organization's experience. *J. Cybersecur., 10*. doi:10.1093/cybsec/tyae013
63. Moussaileb, R., Cuppens-Boulahia, N., Lanet, J.-L., & Bouder, H. L. (2021). A Survey on Windows-based Ransomware Taxonomy and Detection Mechanisms. *ACM Computing Surveys (CSUR), 54*, 1-36. doi:10.1145/3453153
64. Muniandy, M., Ismail, N., Al-Nahari, A., & Yao, D. N. (2024). Evolution and impact of ransomware: Patterns, prevention, and recommendations for organizational resilience. International Journal of Academic Research in Business and Social Sciences, 14. doi:10.6007/IJARBSS/v14-i1/19803
65. Nagar, G. (2024). The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies. *International Journal of Scientific Research and Management (IJSRM)*. doi:10.18535/ijsrm/v12i06.ec09
66. Pattnaik, N., Nurse, J., Turner, S., Mott, G., MacColl, J., Huesch, P., & Sullivan, J. (2023). It's more than just money: The real-world harms from ransomware attacks. *ArXiv, abs/2307.02855*. doi:10.48550/arXiv.2307.02855
67. Perić, J., & Vladimir, C. M. (2019). Demographic, socio-economic and phycological perspective of risk perception from disasters caused by floods: case study Belgrade. *International Journal of Disaster Risk Management, 1*(2), 31-43.
68. Putnik, N. (2022). Sajber rat i sajber mir. Beograd: Akademska misao.
69. Putnik, N., Milošević, M., & Cvetković, V. (2022). Rensomver kao pretnja bezbednosti – društveni i krivičnopravni aspekti. Sociološki pregled, 56(1), 328–353.
70. Rahman, A. M., & Islam, S. (2022). Financial and social costs perspective impacts of cybercrime in the UAE: Policy-guidance addressing the problem in piecemeal approach. International Journal of Economics, Business and Management Studies, 9(2), 89–103. doi:10.55284/ijebms.v9i2.718
71. Rebouh, N., Tout, F., Dinar, H., Benzid, Y., & Zouak, Z. (2024). Integrating Multi-Source Geospatial Data and AHP for Flood Susceptibility Mapping in Ain Smara, Constantine, Algeria. *International Journal of Disaster Risk Management, 6*(2), 245-264.
72. Reshmi, T. (2021). Information security breaches due to ransomware attacks - a systematic literature review. *Int. J. Inf. Manag. Data Insights, 1*, 100013. doi:10.1016/J.JJIMEI.2021.100013
73. Robles-Carrillo, M., & García-Teodoro, P. (2022). Ransomware: An Interdisciplinary Technical and Legal Approach. *Security and Communication Networks*. doi:10.1155/2022/2806605

 doi:10.20944/preprints202504.1950.v1

74. Schwarz, M., Marx, M., & Federrath, H. (2021). A structured analysis of information security incidents in the maritime sector. arXiv preprint arXiv:2112.06545.
75. 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. Preprints. doi:10.20944/preprints202408.2261.v1
76. Singh, H., & Sittig, D. (2016). A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Applied Clinical Informatics, 7*, 624-632. doi:10.4338/ACI-2016-04-SOA-0064
77. Sudheer, S. (2024). Ransomware Attacks and Their Evolving Strategies: A Systematic Review of Recent Incidents. *Journal of Technology and Systems*. doi:10.47941/jts.2399
78. Sviatun, O. V., Goncharuk, O. V., Roman, C., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: Economic and legal aspects. WSEAS Transactions on Business and Economics, 18, 751–762.
79. Tariq, N. (2018). Impact of cyberattacks on financial institutions. Journal of Internet Banking and Commerce, 23(2), 1–11.
80. Tarter, A. (2017). Importance of cyber security. In Community policing – A European perspective: Strategies, best practices and guidelines (pp. 213–230).
81. Thakur, M. (2024). Cyber security threats and countermeasures in digital age. Journal of Applied Science and Education, 4(1), 1–20.
82. ThankGod, J. (2024). Cyber heists and trade turmoil: Uncovering the economic impact of cybersecurity breaches on global commerce. doi:10.2139/ssrn.4858710
83. The Financial Action Task Force. (2023). Countering ransomware financing. FATF. Retrieved from http://www.fatf-gafi.org
84. Umer, S. S. (2024). Analysing in Post COVID-19 era: The Effect of Occupational Stress and Work-Life Balance on Employees Performance. *International Journal of Disaster Risk Management, 6*(1), 75-90.
85. 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. doi:10.13165/IE-24-18-2-02
86. Vibhas, S., Bismark, A. G., Ruiyi, Z., Anwaar, M. A., & Rajib, S. (2019). Understanding the barriers restraining effective operation of flood early warning systems. *1*(2), In press.
87. Vidović, N., Cvetković, V. M., & Beriša, H. (2024). Optimising Disaster Resilience Through Advanced Risk Management and Financial Analysis of Critical Infra-structure in the Serbian Defence Industry. *International Journal of Disaster Risk Management, 6*(2), 183-200.
88. Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: A case study of the Equifax data breach. Issues in Information Systems, 19(3), 66–72.
89. Wang, P., D'Cruze, H., & Wood, D. (2019). Economic costs and impacts of business data breaches. Issues in Information Systems, 20(2), 94–100.
90. Wedawatta, G. (2012). Resilience and adaptation of small and medium-sized enterprises to flood risk. *Disaster Prevention and Management: An International Journal, 21*(4), 474-488. doi:10.1108/09653561211256170
91. Wilner, A., Jeffery, A., Lalor, J., Matthews, K., Robinson, K., Rosolska, A., & Yorgoro, C. (2019). On the social science of ransomware: Technology, security, and society. *Comparative Strategy, 38*, 347-370. doi:10.1080/01495933.2019.1633187
92. Wollerton, M. (2023). Ransomware Attacks. doi:10.4135/cqresrre20230818
93. World Economic Forum. (2024). Global cybersecurity outlook 2024: Insight report. Retrieved from https://www3.weforum.org
94. World Economic Forum. (2025). Global cybersecurity outlook 2025: Insight report. Retrieved from https://reports.weforum.org
95. Yuste, J., & Pastrana, S. (2021). Avaddon ransomware: an in-depth analysis and decryption of infected systems. *ArXiv, abs/2102.04796*. doi:10.1016/j.cose.2021.102388
96. Zimba, A., & Chishimba, M. (2019). On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. *European Journal for Security Research, 4*, 3-31. doi:10.1007/s41125-019-00039-8

 doi:10.20944/preprints202504.1950.v1