Articles

Studia Iuridica Lublinensia vol. 32, 1, 2023
DOI: 10.17951/sil.2023.32.1.191-211

Đorđe Krivokapić
University of Belgrade, Serbia
ORCID: 0000-0002-0950-6820
djordje.krivokapic@fon.bg.ac.rs

Andrea Nikolić
University of Belgrade, Serbia
ORCID: 0000-0001-8739-8717
andrea.nikolic@fon.bg.ac.rs

Aleksandra Stefanović
University of Belgrade, Serbia
ORCID: 0000-0003-0824-0255
aleksandra@ius.bg.ac.rs

Miloš Milosavljević
University of Belgrade, Serbia
ORCID: 0000-0002-4965-4676
milos.milosavljevic@fon.bg.ac.rs

Financial, Accounting and Tax Implications of Ransomware Attack*

Finansowe, bilansowe i podatkowe konsekwencje ataku typu ransomware

CORRESPONDENCE ADDRESS: Đorđe Krivokapić, PhD, Associate Professor, University of Belgrade, Faculty of Organizational Sciences, Jove Ilića 154, 11000 Belgrade, Serbia; Andrea Nikolić, PhD Candidate, Teaching Assistant, University of Belgrade, Faculty of Organizational Sciences, Jove Ilića 154, 11000 Belgrade, Serbia; Aleksandra Stefanović, Teaching Assistant, University of Belgrade, Faculty of Law, King Aleksandar Boulevard 67, 11000 Belgrade, Serbia; Miloš Milosavljević, PhD, Associate Professor, University of Belgrade, Faculty of Organizational Sciences, Jove Ilića 154, 11000 Belgrade, Serbia.

* The article is supported by the European Regional Development Fund (ERDF) project "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ. 02.1.01/0.0/0.0/16_019/0000822).

ABSTRACT

Ransomware is a prime cybersecurity threat at the moment. In this paper we analyze financial implications of ransomware attacks, motivation of the ransomware victim to pay ransom, and legal, accounting and tax implications of such payment. The methodological approach used in the study is a combination of formal-dogmatic method and argumentative literature review. First, we provide an overview of all potential losses which could be incurred by the ransomware attack. Further, we analyze under which conditions is legal to pay any kind of ransom, including cyber ransom, as an organization as well as which other considerations victims should consider when deciding to pay ransom. In that respect we analyze accounting and tax implications of losses inflicted by the ransomware attack, putting special attention to the ransom payments.

Keywords: ransomware; malware; payment; accounting implications

INTRODUCTION

Ransomware cases have exploded in the past few years, thus becoming a cyber-threat that can no longer be ignored.[1] Prior to analyzing financial, accounting, and tax implications of ransomware attack, one should understand what ransomware is. It is a type of malicious software that encrypts and locks victims' data aimed at requesting financial or other compensation. When ransomware occurs, the main dilemma is whether to pay the ransom or not, having in mind that it might be illegal to do so. These, and other topics such as the typology of ransomware attacks, vulnerabilities, attack methodologies, impacts, mitigation, and prevention techniques of the attacks have been vividly discussed in the concurrent body of knowledge.[2] Much less has been known about the financial and taxation implication of ransomware attack.

This paper analyzes the financial implications of ransomware attacks, motivation of the ransomware victim to pay ransom and legal, accounting and tax implications of such payment. The methodological approach used in the study is a combination of formal-dogmatic method and argumentative literature review, to suggest how public policy could support victims without incentivizing attackers to continue with cyber extortion.

The aim of this paper is to address the legality and economic benefit of ransom payment, alongside the coverage of additional costs related to recouping the prior-to-attack business performance of the attacked entity. For this purpose, we used the case of the Republic of Serbia and employed a combination of two methodological approaches – formal-dogmatic method (to analyze positive legal

[1] A. Zimba, M. Chishimba, *On the Economic Impact of Crypto-Ransomware Attacks: The State of the Art on Enterprise Systems*, "European Journal for Security Research" 2019, vol. 4(1), pp. 3–31.

[2] T.R. Reshmi, *Information Security Breaches Due to Ransomware Attacks – a Systematic Literature Review*, "International Journal of Information Management Data Insights" 2021, vol. 1(2).

norms) and scoping review (to address the dilemmas related to the recognition and valuation of the costs for financial, accounting and taxations purposes).

The remainder of the paper is organized in the following order. First, we provide the background of the ransomware attacks on the global scale. Second, we briefly discuss the methods employed in the study and the analyzed legal acts. Third, we thoroughly explain the results of our study. Fourth, we contextualize the results by explaining the key findings, contributions, implications, limitations, and further recommendations.

BACKGROUND TO THE GLOBAL RISE OF RANSOMWARE AND ITS FINANCIAL IMPACT

As internet services and advanced technologies were brought to the masses, so were all sorts of viruses, worms, trojans, and other computer programs specially designed for harm.[3] For the purpose of this paper, special attention is given to the class of cybersecurity threats called malware. Formally defined, malware is "software that harmfully attacks other software, where to harmfully attack can be observed to mean to cause the actual behavior to differ from the intended behavior".[4]

These threats in turn helped advance cryptography: a set of techniques for secure communication in the presence of adversarial behavior traditionally used for solving two kinds of security problems – privacy and authentication. Cryptography had been "for millennia, perceived as a purely protective technology, and in particular as a way to hide the content of messages, secure data at rest, and authenticate users".[5] By moving beyond linguistic and lexicographic patterns of the classical age, modern cryptography has made extensive use of mathematical subdisciplines, including computational complexity, abstract algebra and finite mathematics.

In the 1990s a proposal for merger of ideas was made – two separate fields brought together, malware and cryptography, offered a glimpse into a formidable threat: malicious software weaponizing cryptography as an attack tool, enabling the attacker to take control of the targeted data without accessing or extracting it. This hybrid field is called cryptovirology and it now studies crypto viruses, cryptoworms, crypto trojans and alike, computer software designed to encrypt victim's data and render it unavailable. If the attacker offers a chance for decryption, it comes with

[3] N. Karpiuk, *Blockchain as a Non-Standard Response to the Limitation of Positive Law in the Social Media Environment*, "Studia Iuridica Lublinensia" 2021, vol. 30(5), pp. 295–307.

[4] S. Kramer, J.C., Bradfield, *A General Definition of Malware*, "Journal in Computer Virology" 2009, vol. 6(2), pp. 105–114.

[5] A.L. Young, M. Yung, *Cryptovirology*, "Communications of the ACM" 2017, vol. 60(7), pp. 24–26.

a price. In this new relatively novel extortion model widely known as ransomware, the attackers offer to encrypt an organization's data and demand payment to enable restoring access to data.

In recent years, ransomware attackers completely changed the "business" model on which they operate. Namely, they do not steal and sell data, as they used to do before, but it is sufficient that they threaten to do so or to simply lock the victim's data. It became very profitable for attackers, especially due to the evolution of crypto payment methods that are anonymous.

According to the 2021 ENISA Threat Landscape Report ransomware has been the prime threat during the reporting period, with several high profile and highly publicized incidents.[6] The rapid increase in volume, frequency and cost of ransomware attacks, created the environment in which it cannot be considered as an unforeseeable risk. Still, reliable statistics are hard to get, as the ransomware reporting practice is not steady. However, some of the available reports, which base their data on available insurance claims related to the ransomware attacks, show that reimbursements for ransomware have grown in recent years from 22% in 2019 to 30% in 2020,[7] whilst there is a 72% increase in the number of ransomware attacks since the beginning of the COVID-19 pandemic.[8]

Ransomware attacks used to be directed against individuals with unprotected information systems, but nowadays a victim of a ransomware attack could be literally anyone – from a small private company to a large organization fully equipped with information systems protection. Public authorities are not spared, and in recent cases, attackers' targets were ministries, hospitals, geodetic authorities, etc. Recent research is showing that the most impacted industries are professional services (21.9%), public sector (14.4%), health care (10.0%) and software services (9.4%).[9] Nonetheless, many national cybersecurity systems in Europe have reported that "the scale, frequency, and impact of cybersecurity incidents is growing".[10]

The Western Balkan region recently had a rise in ransomware attacks targeting the public sector. In June 2022, the Serbian Republic Geodetic Authority respon-

---

[6] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2021*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (access: 27.10.2022).

[7] D. Pain, D. Noordhoek, *Ransomware: An Insurance Market Perspective*, July 2022, https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/ransomware_web.pdf (access: 15.11.2022).

[8] S. Rauch, *The Rise of Ransomware in the Era of Covid-19*, 28.10.2021, https://www.simplilearn.com/rise-of-ransomware-in-the-era-of-covid-article (access: 16.11.2022).

[9] CoveWare, *Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022*, 28.7.2022, https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022 (access: 15.11.2022).

[10] K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *Introduction*, [in:] K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021.

sible for registration of rights to real estate was hit by a ransomware attack that prevented access to regular services disabling many citizens to change the real estate ownership in the registry.[11] Attacks have been reported in other countries in the regions, including the following institutions: the Ministry of Agriculture and the Ministry of Science and Education of the Republic of North Macedonia, the Parliament of Bosnia and Herzegovina and the Council of Ministers of Bosnia and Herzegovina, various public institutions in Albania, and almost complete governmental IT structure of Montenegro.

As the number of reported ransomware attack cases increase in the West Balkan region, this paper aims at exploring the legality and economic benefit of ransom payment, alongside the coverage of additional costs related to recouping the prior-to-attack business performance of the attacked entity. The Serbian setting is selected for the analysis, but the findings can, to some extent, be interesting to other West Balkan countries as well.

METHODS

To address the purpose, this study combines two methodological approaches. The first one is based on the formal-dogmatic method.[12] This method is based on logical analysis, argumentation, and hermeneutics of the legal norms in Serbia and other legal systems associated with ransomware attacks and ransom payments. Thus, this method allows *de lege lata* and *de lege ferenda* interpretations and discussion.[13] The set of legal documents includes:

- Conceptual Framework for Financial Reporting 2018,
- Law on Accounting and Auditing,
- Law on Corporate Profit Tax,
- Rulebook on Chart of Accounts,
- Law on Value Added Tax,
- Rulebook on Value Added Tax,
- Law on Digital Property,

[11] Republic Geodetic Authority (RGZ), *IT infrastruktura RGZ meta intenzivnog hakerskog napada*, 15.6.2022, https://www.rgz.gov.rs/vesti/5028/vest/it-infrastruktura-rgz-a-meta-intenzivnog-hakerskog-napada (access: 15.11.2022).

[12] I. Hoffman, J. Kostrubiec, *Political Freedoms and Rights in Relation to the COVID-19 Pandemic in Poland and Hungary in a Comparative Legal Perspective*, "Białostockie Studia Prawnicze" 2022, vol. 27(2), pp. 31–53.

[13] J. Kostrubiec, *The Role of Public Order Regulations as Acts of Local Law in the Performance of Tasks in the Field of Public Security by Local Self-government in Poland*, "Lex localis – Journal of Local Self-Government" 2021, vol. 19(1).

- Law on Obligations,
- Criminal Code,
- Law on Personal Data Protection,
- Law on Information Security.

The second method is scoping review. To answer dilemmas related to the financial, accounting, and taxation issues arising from the incomplete legal framework, we used scholarly and practical reports and studies on ransomware incidents. For this purpose, the Web of Science database was used, as it provides the most comprehensive scope for search.[14]

RESULTS

According to the *Conceptual Framework for Financial Reporting*, expenses are "decreases in economic benefits during the accounting period in the form of outflows or depletions of assets or incurrences of liabilities that result in decreases in equity, other than those relating to distributions to equity participants".[15] Expense should be recognized and valued in the income statement once the economic benefits for the reporting entity occur.

Looking through the lens of ransomware attack payment, this standard-related definition of expense implies that any decrease in economic benefits should be recognized once the payment has been made to the attacker. This, however, brings about a myriad of different dilemmas:

1. What are the potential losses which could be incurred by the ransomware attack?
2. Is there an economic benefit of paying ransom?
3. Is ransomware payment legal?
4. What is the legal qualification of such payment?
5. Which costs related to the ransomware attack should be viewed as expenses, and which ones are solely opportunity costs without any real possibility to be recognized in financial or taxation reporting?
6. What is payment typology and valuation?

To provide the answer to these interrogatives, we first provide an overview of all potential losses when ransomware occurs. Afterward, we elaborate on the economic benefit of paying ransom, then dissect the legality and legal qualification of ransom-

[14] Z. Spasenic, M. Milosavljevic, N. Milanovic, *Project Financing of Renewable Energy Projects: A Bibliometric Analysis and Future Research Agenda*, "Fresenius Environmental Bulletin" 2022, vol. 31(8), pp. 7844–7851.

[15] International Accounting Standards Board, *Conceptual Framework 2018*, https://www.ifrs.org/projects/completed-projects/2018/conceptual-framework (access: 10.11.2022).

ware payment. Further, we address cost structure of ransomware protection, attacks and payment, and payment typology. Finally, we provide potential recommendations based on epistemology gathered from the concurrent body of knowledge.

1. Overview of losses which could be incurred by the ransomware attack

Ransomware can cause considerable negative consequences for the victim, including non-recuperation and recoverable costs. Different types of damages that can occur, encompass financial loss including ransom payment and recovery process, operating loss caused by business discontinuity, data loss caused by data breach, which would be addressed in detail below. However, ransomware can affect third parties as well, triggering liability claims for loss suffered by third parties, loss of customers, reputational damage, etc.[16]

All mentioned losses could be divided into three categories: (1) incident response costs, which might include a ransomware payment, (2) costs related to business discontinuity, and (3) third party claims.

Incident response costs include expert assistance IT recovery, legal and communication perspectives. If the victim decides not to pay ransom and recover the system on their own, the recovery process would be extensive and include investigation costs, verification costs to check systems (diagnosis and remediation), restoration costs to put systems back online (testing).

Business discontinuity costs include a range of operational costs, like loss of customers, loss of reputation, data loss as an operating loss caused by business discontinuity, which could have severe consequences depending on the industry.

Finally, third party claims could vary from a data breach claim made by a third party to a claim for compensating other type of damages suffered by a third party, including material and non-material (e.g. death) damage.

Table 1. Direct and indirect losses related to ransomware attack

Direct losses related to ransomware attack	Indirect losses related to ransomware attack
Ransom payment	Recovery process: – investigation costs – verification costs to check systems (diagnosis and remediation) – restoration costs to put systems back online (testing)
Data breach claims by third parties	Data loss as an operating loss caused by business discontinuity
Other liability claims for loss suffered by third parties	Loss of customers
Market value or replacement value of the property destroyed or services	Loss of reputation

Source: own elaboration.

[16] Đ. Krivokapić, A. Nikolić, *Legal Obligations and Liability in a Ransomware Attack*, "Zbornik radova Kopaoničke škole prirodnog prava – Slobodan Perović" 2022, vol. 3, pp. 173–196.

2. Economic benefit of paying ransom

The recent study finds that "victims often weigh the costs and benefits of interventions before making final decisions, and that their decisions are based on a range of reasons".[17] To dig deeper into the approaches to ransomware attack payment treatment, an interesting point of view is given in the study of D. Dey and A. Lahiri.[18] This study uses a game-theory model to explain whether a government should ban ransomware attack payments. The resulting equilibrium indicates that in some cases banning may be ineffective in providing general public welfare. Consequently, banning such payments is a sub-optimal decision in some cases. This, however, does not imply whether that ransomware payment should be recognized as an expense, but only argues that ransom payment does not provide economic welfare outside of the victim organization.

On the other hand, it is a bit controversial that the French Treasury recommends insurance companies to cover the ransoms paid by victims of cyberattacks, and that the French Government will further develop a stimulating framework for this type of insurance.[19] Such an approach has financial justification if a victim has commercial insurance against ransomware attacks and there is an incident in which the requested ransom has a smaller value compared to recovery and other potential costs which is usually the case because the "cost of downtime is typically 5–10x the actual ransom amount".[20]

If ransomware risk could be covered, the insurance companies might include provisions in insurance policies that they will reimburse the cost of the ransom demand together with the risk that the transaction will not be successful, or the cost of rebuilding the system – whichever is lower.[21]

3. Legality of ransomware payment

Although it is a contemporary and innovative type of attack, ransomware as a cybersecurity risk is already covered by existing legal regulations, primarily in the areas of cybercrime, information security, and data protection, but also in

[17] A. Yuryna Connolly, H. Borrion, *Reducing Ransomware Crime: Analysis of Victims' Payment Decisions*, "Computers and Security" 2022, vol. 119.

[18] D. Dey, A. Lahiri, *Should We Outlaw Ransomware Payments?*, [in:] *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2021.

[19] T. Labro, *Ransomware, la nouvelle doctrine française*, 23.9.2022, https://paperjam.lu/article/ransomware-nouvelle-doctrine-f (access: 16.11.2022).

[20] C. Mehra, A.K. Sharma, A. Sharma, *Elucidating Ransomware Attacks in Cyber-Security*, "International Journal of Innovative Technology and Exploring Engineering" 2019, vol. 9(1).

[21] M. Rasch, *States Prohibit Ransomware Payments*, 8.7.2022. https://securityboulevard.com/2022/07/states-prohibit-ransomware-payments (access: 16.11.2022).

various sectoral regulations applicable to specific sectors.[22] As a type of malware, ransomware is incriminated by "Data interference" and "System interference" criminal offenses established by Budapest Convention on Cybercrime, while national legal systems in practice complement these provisions with other criminal offenses such as extortion, ransom and coercion as well as national offenses related to cybercrime.[23]

Performing ransomware attacks is illegal, as well as financially demanding compensation to provide decryption keys, but what about paying ransom by the victim? It seems that limitations on paying ransom could be imposed by internal policies of organization and public order.

Victims are generally not forbidden to negotiate with criminals in cases of ransom and extortion. Payment of ransom is a decision to be made solely by the victim and law enforcement officials could advise on ransom payment, but will not make the final decision as to paying or not.[24] Some evidence indicate that organizations are more willing to pay the hacker's ransom than invest in information security,[25] whilst 60% of global ransom targets paid ransom, 44% in Europe, which is a pretty high number.[26]

Prohibiting victims from paying ransom is quite a controversial issue. Although the ransom ban could potentially push attackers from ransom tactics, it is unlikely that such an approach would impact cyber criminals in a manner that they would stop with attacks while it would put targets into even more difficult positions.[27] Therefore, the report recommended a gradual approach which would involve prohibitions over time, initially applicable only to specific sectors, but with a strong protection and support program for the victims.[28]

The first such ban was imposed in mid-2021 by North Carolina who prohibited the public sector from paying ransom or even negotiating with criminals behind ransomware attacks.[29] Similar policies have been followed by Florida in

[22] Đ. Krivokapić, A. Nikolić, *op. cit.*, pp. 173–196.

[23] N. Putnik, M. Milošević, V. Cvetković, *Ransomware as a Security Threat: Social and Criminal Legislation Aspects*, "Socioloski Pregled" 2022, vol. 56(1), pp. 328–353.

[24] J.F. Broder, E. Tucker, *Risk Analysis and the Security Survey*, Oxford 2012.

[25] P. Leo, Ö. Isik, F. Muhly, *The Ransomware Dilemma*, "MIT Sloan Management Review" 2022, vol. 63(4), pp. 13–15.

[26] Claroty, *The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption*, 2021, https://security.claroty.com/report/global-state-industrial-cybersecurity-survey-2021 (access: 16.11.2022).

[27] Ransomware Task Force, *Combating Ransomware*, 2021, https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf (access: 16.11.2022).

[28] *Ibidem*.

[29] B. Freed, *North Carolina Moves Toward Ban on Ransomware Payments*, 14.5.2021, https://statescoop.com/north-carolina-moves-toward-ban-on-ransomware-payments (access: 16.11.2022).

mid-2022[30] and are considered by four additional US states[31] and Australia.[32] Although European governments usually publicly advocate against paying ransom, there is no serious initiative to ban it.

At the same time, 70% of targets are of the opinion that ransomware payments should be legal (28% regardless of notification, 41% as long as the ransom payment is reported),[33] while the practitioners are generally equivocal in advocating the avoidance of ransom payment. First, such a payment is seen as unethical as it will only fund continued criminal activity, and risky – since in approximately 29% of cases entities have never gained access to their data after paying ransom.[34] The latter one is particularly relevant for our study since it drains the certainty of economic benefits of ransom payment for the victim organization.

Beside the possible explicit prohibition of ransom payment, there are additional regulatory regimes which could still incriminate paying ransom under certain circumstances: anti-money laundering regulation, counter-terrorism regulation, and international sanctions regimes. That would be the case when attackers are terrorist organizations or actors designated on international sanction lists. Although, the enforcement procedure against the victim that paid ransom is not prescribed, and it is unlikely that this issue could be regulated, due to the absence of evidence that a ransom is paid to actor to whom the prohibition of payment is established by these regulatory frameworks, the organization should consider these risks and take steps to mitigate them if they decide to pay a ransom. The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury provided guidance which targets involved in the payment of ransoms have to follow in order to try to ensure the legality of any such payments in the context of sanctions risks.[35] Major considerations in such cases are: whether the target organization previously took steps to reduce cybersecurity risks and whether it reports ransomware attacks as soon as possible and further cooperates on the issue with relevant government agencies.

---

[30] E. Elam, B. Wange, *Florida Follows North Carolina in Prohibiting State Agencies from Paying Ransoms*, 23.7.2022, https://www.databreaches.net/florida-follows-north-carolina-in-prohibiting-state-agencies-from-paying-ransoms (access: 16.11.2022).

[31] M. Rasch, *op. cit*.

[32] S. McKeith, *Australia to Consider Banning Paying of Ransoms to Cyber Criminals*, 14.11.2022, https://www.reuters.com/technology/australia-consider-banning-paying-ransoms-cyber-criminals-2022-11-12 (access: 16.11.2022).

[33] Claroty, *op. cit*.

[34] T. Slattery, G. Kirrane, *How to Manage the Risk of a Ransomware Attack*, 20.5.2021, https://www.ey.com/en_ie/cybersecurity/how-to-manage-the-risk-of-a-ransomware-attack (access: 17.10.2022).

[35] Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, 21.9.2021, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf (access: 17.11.2022).

4. Legal qualification of ransomware payment

From a private law point of view, the victim agrees to make ransomware payment in exchange for decryption keys being provided by the attacker. Such non-monetary obligations are usually done in cryptocurrency. The most preferred cryptocurrency for this type of transaction is Bitcoin participating with 98% in total share of ransomware payout transactions.[36] Bitcoin's exchange system is based on peer-to-peer networking without any need for intermediary. Thus, it is significantly difficult to trace the payment and find the affiliation of the attacker. The payment patterns are discerning and hard to forensically investigate.[37] Some companies have even started stockpiling digital cash because of the rise of ransomware, and empirical evidence indicates unidirectional ties between the prevalence of ransomware and Bitcoin.[38]

However, due to the existence of extortion and threats, the execution of the contract is a criminal act[39] and by so, the contract is void. Since it is void, to speak of a contract is *contradictio in adjecto*, and therefore the payment is payment of indue. Victim here knew the reason for paying but was under threat. In general, possessing knowledge of paying of indue would lead to absence of restitution, but illegal threat of a private person replaces error as a condition for the payment of indue compared to the legal threat of a public person (e.g. paying residual tax).

On the practical side, the victim decides to accept the attackers offer and to pay ransom. In order to perform, the victim needs to obtain cryptocurrency and transfer it to the designated crypto wallet. Obtaining cryptocurrency usually requires transfer of hard currency into it. Cryptocurrency is an investment into digital asset.[40] After the transfer in ransomware payment is performed digital assets are (a) transformed again into hard currency or (b) held in a crypto wallet of the attacker.

From a legal and ethical point of view, the victim should officially report the ransomware attack under criminal, information security and sometimes data protection regulations.[41] Such reporting obligation is not clearly established regarding

[36] C. Mehra, A.K. Sharma, A. Sharma, *op. cit*.

[37] A.B. Turner, S. McCombie, A.J. Uhlmann, *Discerning Payment Patterns in Bitcoin from Ransomware Attacks*, "Journal of Money Laundering Control" 2020, vol. 23(3).

[38] H. Lee, K.-S. Choi, *Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework*, "Victims and Offenders" 2021, vol. 16(3).

[39] Đ. Krivokapić, A. Nikolić, *op. cit.*, pp. 173–196.

[40] S. Trimborn, M. Li, W.K. Härdle, *Investing with Cryptocurrencies – a Liquidity Constrained Investment Approach*, "Journal of Financial Econometrics" 2019, vol. 18(2); J. Liew, R. Li, T. Budavári, A. Sharma, *Cryptocurrency Investing Examined*, "Journal of the British Blockchain Association" 2019, vol. 2(2), pp. 1–12; D. Xi, T.I. O'Brien, E. Irannezhad, *Investigating the Investment Behaviors in Cryptocurrency*, "Journal of Alternative Investments" 2020, vol. 23(2), pp. 141–160.

[41] Đ. Krivokapić, A. Nikolić, *op. cit.*, pp. 173–196.

a ransomware payment. However, it is unlikely that the authorities would attribute, stop, and bring to justice attackers.[42] Therefore, the victim cannot expect that the payment will be returned to it via adhesional part of criminal proceedings. From a private law point of view, due to the voidance, the victim is authorized to ask for the restitution of the payment of undue. Such a legal request is not effective because the attacker is protected by its anonymity. As a result of a decision to pay ransom, regardless of the success of the transaction and potential data recovery, the victim is left without digital assets but with a substitute of the unrecoverable claim.

The ransomware payment could also be approached as: a gift, an investment (capital expenditure), and theft. However, the gift is a unilateral non-monetary obligation, but there is no *animus donandi* upon payment of ransom. An investment is a mechanism for generic future profit, while reasons for paying ransomware are establishing business continuance and avoiding additional damages. Therefore, ransom payment cannot be qualified as a capital expenditure, because it is not creating an asset with either a definite or indefinite useful life that could produce added value in future years.[43] The theft is stealing of other persons' property with the intention to obtain unlawful material gain. The theft implies that a victim is not contributing to the act of theft. However, the transfer of Bitcoin in ransom payment is done willingly while some companies even stockpile crypto in anticipation of ransomware attacks.[44]

5. Cost structure of ransomware protection, attacks, and payment

Every ransomware attack has its own peculiarities. The same goes for the economic benefit of paying ransom and the cost structure of ransomware attacks. A handful of attempts have hitherto been made to justify any of the payments related to ransomware attacks. From a grand scheme of things, this payout is a subclass of extortion from the economics perspective.

As it has been already mentioned above, ransom payment is only one of the costs that victims may face. In fact, the victims of ransomware attacks are facing numerous losses, while only some of the costs could be mitigated by paying the ransom. If an organization decides to recover without ransom payment, the recovery

[42] A. Peters, A. Jordan, *Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime*, "Journal of National Security Law and Policy" 2020, vol. 10, pp. 487–524.

[43] D.T. Williamson, A.B. Staley, *Ransomware: Tax Compliance Issues for a New Reality*, "Tax Management Memorandum" 2017, vol. 58(12), p. 281.

[44] F. Donovan, *CISOs Stockpile Cryptocurrency in Case of Ransomware Attack*, 25.7.2018, https://healthitsecurity.com/news/cisos-stockpile-cryptocurrency-in-case-of-ransomware-attack (access: 16.11.2022).

costs will be higher and they might include support of external support like forensic reviewers, and the reconstruction of the IT system.[45]

From the point of view of loss recognition, some costs being actual and possibly recognizable in the income statement while other being implicit by nature,[46] as shown in Table 2.

Table 2. Loss recognition from cyberattacks

Recuperation costs (recognizable)	Non-recuperation costs (non-recognizable)
Verification costs to check systems (diagnosis and remediation)	Lost profits
Restoration costs to put systems back online (testing)	Reasonable value of loss caused by "unavailability"
Market value or replacement value of the property destroyed or services	Investigation costs
	Past or future losses
	Injury suffered
	Loss of computer time (lost productivity)

Source: G.S. Smith, *Recognizing and Preparing Loss Estimates from Cyber-Attacks*, "Information Systems Security" 2004, vol. 12(6).

When it comes to non-recuperation costs in cases of ransomware attacks, they are usually related to all the resources that require sacrifice to allow the company to "bounce back" to the pre-attack position. This cost of downtime is measured in lost productivity which includes sluggish labor, lost revenue opportunities, and loss of goodwill.[47]

However, the one type of cost that requires special attention in respect to the accounting and tax-related recognition is ransomware payment, even though it can go as much as $4 billion.[48] According to the analysis made above, it is justifiable to qualify ransom payment as payment in respect to the void contract, payment of indue, and theft and damages incurred by the criminal act.

With the ransom paid, the company must face decisions regarding the proper treatment of the payment on its books and ultimately its tax return. If the victim does not have accumulated crypto ready to be used for the payment he or she will first need to buy some that would be treated as an investment into digital assets. After the payment, the victim is faced with the challenge to justify change in the equity and make it tax deductible.

[45] C. Mehra, A.K. Sharma, A. Sharma, *op. cit.*

[46] G.S. Smith, *Recognizing and Preparing Loss Estimates from Cyber-Attacks*, "Information Systems Security" 2004, vol. 12(6).

[47] C. Mehra, A.K. Sharma, A. Sharma, *op. cit*.

[48] X. Wang, B. An, H. Chan, *Who Should Pay the Cost: A Game-Theoretic Model for Government Subsidized Investments to Improve National Cybersecurity*, [in:] *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence*, 2019.

Recognition of a particular asset or liability and any resulting income, expenses or changes in equity requires documented evidence and the high probability of economic benefits.[49] In the USA the victim could treat ransom payment as a nondeductible illegal payment, a deductible theft loss under, or even an ordinary or necessary trade or business expense.[50] From the Serbian accounting perspective, the victim could try to recognize ransomware payment as recuperation cost as a shortage or loss of assets (574), writing-off of receivables (575), and other business expenses (579) (Rulebook on Chart of Accounts). Due to the non-existence of the valid business transaction, we are of the opinion that the ransomware payment cannot be classified as a regular business expense under categories 50 to 55.

According to Law on Corporate Profit Tax (§ 16) the written off value of uncollectible receivables can be recognized as expenditures, on condition that: 1) such receivables were previously included in the taxpayer's revenues; 2) have been written off in the taxpayer's books as uncollectible; and 3) if evidence is presented on failed collection of such receivables based on legal proceedings. Considering that the victim after the ransom payment can transfer its assets from digital property into the receivable toward the attacker based on the payment of undue, it would be possible to use this option. The absence of legal proceedings which could evidence failed collection due to the anonymity of the attacker could limit the victim in this respect, except if the unsuccessful criminal proceeding would be recognized as sufficient evidence. Otherwise, the victim could adjust the value of uncollectible receivables which could be recognized as a charge to expenditures if at least 60 days have expired from the deadline for their collection, without any additional conditions.

Law on Corporate Profit Tax does not directly deal with shortage or loss of assets, but the Rulebook on Chart of Accounts (§ 40) provides that shortages could be recoverable under certain conditions but does not provide any guidance regarding digital assets. As per Law on Value Added Tax (§ 4) and Rulebook on Value Added Tax (§ 8), losses made on assets can be tax deductible if it was affected by force majeure or other justifiable reason. The definition of force majeure is, nonetheless, ambiguous. Theft and extortion (unlike nature-caused disasters) are not specified as force majeure, but a number of official opinions of Ministry of Finance (430-00-00446/2018-04 as of 12 February 2020; 011-00-48/2018-04 as of 5 June 2018; and 413-00-2174/2009-04 as of 14 September 2009) do recognize theft as other justifiable reason. Accordingly, the practice allows victims to treat theft and potentially ransom payment as loss, but it has to be documented based on the act of the competent authority or organizations (i.e. police and prosecution). By

[49] International Accounting Standards Board, *op. cit*.
[50] D.T. Williamson, A.B. Staley, *op. cit.*, p. 281.

analogy, it could be argued that loss of assets due to the theft and extortion could be recognized as an expense under corporate profit tax regulation.

Special conditions for deduction of "other business expenses" are not established under Serbian legal regulation. Therefore, it is not entirely clear would it be possible to deduct ransom payment under this category but we are of the opinion that there are no major obstacles if economic benefit of paying ransom could be proved and documentation regarding ransomware attack and ransomware payment could be presented in accordance with other applicable regulations because the loss happens as a side effect of business.

6. Payment typology and valuation

Another dilemma in case of a ransomware payment is the valuation of the expense and the commercial documents that itemizes and records the economic transaction (ransom payment).

This is partially affected by the payment method. All ransom payment are categorizes as (1) direct and (2) indirect.[51] As for the direct payment methods – the dominant algorithm is payment in cryptocurrencies. The rationale is straightforward: "The in-built anonymity of cryptocurrency networks makes this virtual asset a perfect biotope to shelter and trade in the proceeds from illegal activities".[52] Regarding the indirect payment method – usual forms include "pre-paid voucher cards, online product purchases as well as calls to premium rate".[53] B. Custers, J.-J. Oerlemans and R. Pool elaborated on the mechanics of voucher payment.[54] These vouchers are first bought and then resold on auction sites such as eBay, and the unfortunate buyer must deal with the consequences. Similar approach is used for prepaid services such as "Ukash", "Paysafecard" or "Moneypak", where such gifts are auctioned after the transfer.[55] Short message service (SMS) or calls to premium rates are favorable mechanisms for mobile lockers.

The payment topology latently affects the valuation of the loss in assets. Any asset previously acquired by the company is usually valued on a historical basis (purchase costs). The same goes for cryptocurrencies and vouchers. At the time

[51] I. Nadir, T. Bakhshi, *Contemporary Cybercrime: A Taxonomy of Ransomware Threats and Mitigation Techniques*, International Conference on Computing, Mathematics and Engineering Technologies (ICoMET) 2018.

[52] See T. Falcao, B. Michel, *Taxation of Cryptocurrencies*, "SSRN Electronic Journal" 2022, pp. 11–41.

[53] I. Nadir, T. Bakhshi, *op. cit*.

[54] B. Custers, J.-J. Oerlemans, R. Pool, *Laundering the Profits of Ransomware*, "European Journal of Crime, Criminal Law and Criminal Justice" 2020, vol. 28(2), pp. 121–152.

[55] P. O'Kane, S. Sezer, D. Carlin, *Evolution of Ransomware*, "IET Networks" 2018, vol. 7(5), pp. 321–327.

of the recognition of the loss (the actual payment date), the loss might be higher or lower than the historical value of the purchase. However, with regard to stable digital assets (see § 2 of the Law on Digital Assets) – the value is supposed to be stable over time without actual fluctuations. As for the non-dominant payment method (i.e. SMS-based payment), the value of loss should be recognized as an ongoing cost.

It is interesting to point out that ransomware payment performed via cryptocurrency which is obtained by the victim prior to the ransom attack would be subject to the capital gain tax in accordance with Law on Corporate Profit Tax (§ 27).

DISCUSSION AND CONCLUSIONS

The aim of this paper is to address the legality and economic benefit of ransom payment, alongside the coverage of additional costs related to recouping the prior-to-attack business performance of the attacked entity. For this purpose, we used the case of the Republic of Serbia and employed a combination of two methodological approaches – formal-dogmatic method (to analyze positive legal norms) and scoping review (to address the dilemmas related to the recognition and valuation of the costs for financial, accounting and taxations purposes). The main findings of our study indicate that ransom payment is (still) not illegal, and can be approached as a payment of indue, gift, investment (capital expenditure), and theft. Nonetheless, the payment cannot be recognized for financial or taxation reporting purposes and, thus, it is subject to a number of taxations.

As ransomware attacks become more frequent, organizations should develop adequate internal cyber policies that would minimize the impact of ransomware. Moreover, they have a duty to comply with a set of *ex ante* obligations prescribed in different legal regulations. Prevention is the key, so the recommendation for organizations, i.e. potential victims, is to undertake a general cybersecurity risk assessment, especially examining risks associated with ransomware, to form an incident response team, to educate the team, and to take other organizational and technical measures to minimize potential risks.[56]

When the legality is met as a substantial criterion, we move towards the recognition and valuation issues related to the costs of ransomware attacks. Recognition of a particular asset or liability and any resulting income, expenses or changes in equity requires. According to the positive legislation in Serbia, the ransomware payment cannot be classified as a regular business expense, as documented evidence is required for recognition of a particular asset or liability. As an alternative, the victim could try to recognize ransomware payment as recuperation cost as a shortage

[56] Đ. Krivokapić, A. Nikolić, *op. cit.*, pp. 173–196.

or loss of assets, writing-off of receivables, and other business expenses. Several issues leading to the extensive taxation remain unresolved. First, the unrecognized loss in assets may lead to VAT taxation. If the payment is made from the previously stockpiled digital assets, the entity may be a subject of capital gains taxation. Then, the unrecognized business loss may lead to corporate gains taxation. When other cost elements (required to fully recover the business processes) are added to the equation, a simple ransom attack becomes an important bankruptcy-leading phenomenon.

To achieve the legality and be able to eventually deduct ransom payment as an expense organization should:

- undertook a general cyber security risk assessment, especially examining risks associated with ransomware, and complied with any applicable regulation, cybersecurity standards, and best practices,
- notify all the relevant actors, including financial institutions, about the ransom attack and about the payment of the ransom,
- verify that they did not breach other sectoral regulations (AML&CT, sanctions, other financial regulations),
- prepare a crisis management analysis which concludes that ransom payment could significantly reduce losses and provide economic benefit to the organization compared to the system recovery without the description.

Notification of all the relevant actors, including financial institutions, about the ransom attack and about the payment of the ransom should be critical for successful deduction of ransom payment since such modification would produce sufficient documented evidence.

In addition to the possibility of claiming tax deductions, organizations should invest in insurance policy coverage that would encompass cybersecurity insurance apart from general commercial policies.[57] That way organizations would be fully protected from the ransomware attack and would be able to recover costs related to it.

Finally, since states are not capable to effectively protect themselves from ransomware attacks it would be recommended that states encourage investments into cyber security posture. Such investment could be expedited if the tax authorities would introduce double deduction of such costs (see § 22g of the Law on Corporate Profit Tax, related to research and development costs).

Ransomware attacks are globally rising and none of the organizations is excluded from the list of potential victims. This study adds to the concurrent body of knowledge on cybersecurity by delineating the financial, accounting, and taxation treatment of the ransom payment in the context of the Republic of Serbia.

[57] E. Galinkin, *Winning the Ransomware Lottery: A Game-Theoretic Approach to Preventing Ransomware Attacks*, [in:] *Lecture Notes in Computer Science*, 2021, pp. 195–207.

This study has several potential flaws. To name a few, the legal analysis is conducted solely in the context of a single country. An avenue for further research is related to cross-country studies. These studies should be easily motivated – crime does not recognize borders, neither should scholars examining such crime. Second, the study deals only with a paucity of possible effects of ransomware payments. Future research projects should encompass factors such as the ethics or cost-effectiveness of payments.

REFERENCES

Literature

Broder J.F., Tucker E., *Risk Analysis and the Security Survey*, Oxford 2012.

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *Introduction*, [in:] K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021, **DOI: https://doi.org/10.4335/2021.5**.

Custers B., Oerlemans J.-J., Pool R., *Laundering the Profits of Ransomware*, "European Journal of Crime, Criminal Law and Criminal Justice" 2020, vol. 28(2), **DOI: https://doi.org/10.1163/15718174-02802002**.

Dey D., Lahiri A., *Should We Outlaw Ransomware Payments?*, [in:] *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2021, **DOI: https://doi.org/10.24251/hicss.2021.794**.

Falcao T., Michel B., *Taxation of Cryptocurrencies*, "SSRN Electronic Journal" 2022, **DOI: https://doi.org/10.2139/ssrn.4193099**.

Galinkin E., *Winning the Ransomware Lottery: A Game-Theoretic Approach to Preventing Ransomware Attacks*, [in:] *Lecture Notes in Computer Science*, 2021, **DOI: https://doi.org/10.1007/978-3-030-90370-1_11**.

Hoffman I., Kostrubiec J., *Political Freedoms and Rights in Relation to the COVID-19 Pandemic in Poland and Hungary in a Comparative Legal Perspective*, "Białostockie Studia Prawnicze" 2022, vol. 27(2), **DOI: https://doi.org/10.15290/bsp.2022.27.02.02**.

Karpiuk N., *Blockchain as a Non-Standard Response to the Limitation of Positive Law in the Social Media Environment*, "Studia Iuridica Lublinensia" 2021, vol. 30(5), **DOI: https://doi.org/10.17951/sil.2021.30.5.295-307**.

Kostrubiec J., *The Role of Public Order Regulations as Acts of Local Law in the Performance of Tasks in the Field of Public Security by Local Self-government in Poland*, "Lex localis – Journal of Local Self-Government" 2021, vol. 19(1), **DOI: https://doi.org/10.4335/19.1.111-129(2021)**.

Kramer S., Bradfield J.C., *A General Definition of Malware*, "Journal in Computer Virology" 2009, vol. 6(2), **DOI: https://doi.org/10.1007/s11416-009-0137-1**.

Krivokapić Đ., Nikolić A., *Legal Obligations and Liability in a Ransomware Attack*, "Zbornik radova Kopaoničke škole prirodnog prava – Slobodan Perović" 2022, vol. 3.

Lee H., Choi K.-S., *Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework*, "Victims and Offenders" 2021, vol. 16(3), **DOI: https://doi.org/10.1080/15564886.2020.1835764**.

Leo P., Isik Ö., Muhly F., *The Ransomware Dilemma*, "MIT Sloan Management Review" 2022, vol. 63(4).

Liew J., Li R., Budavári T., Sharma A., *Cryptocurrency Investing Examined*, "Journal of the British Blockchain Association" 2019, vol. 2(2), **DOI: https://doi.org/10.31585/jbba-2-2-(2)2019**.

Mehra C., Sharma A.K., Sharma A., *Elucidating Ransomware Attacks in Cyber-Security*, "International Journal of Innovative Technology and Exploring Engineering" 2019, vol. 9(1), **DOI: https://doi.org/10.35940/ijitee.A8106.119119**.

Nadir I., Bakhshi T., *Contemporary Cybercrime: A Taxonomy of Ransomware Threats and Mitigation Techniques*, International Conference on Computing, Mathematics and Engineering Technologies (ICoMET) 2018, **DOI: https://doi.org/10.1109/icomet.2018.8346329**.

O'Kane P., Sezer S., Carlin D., *Evolution of Ransomware*, "IET Networks" 2018, vol. 7(5), **DOI: https://doi.org/10.1049/iet-net.2017.0207**.

Peters A., Jordan A., *Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime*, "Journal of National Security Law and Policy" 2020, vol. 10.

Putnik N., Milošević M., Cvetković V., *Ransomware as a Security Threat: Social and Criminal Legislation Aspects*, "Socioloski Pregled" 2022, vol. 56(1), **DOI: https://doi.org/10.5937/socpreg56-36845**.

Reshmi T.R., *Information Security Breaches Due to Ransomware Attacks – a Systematic Literature Review*, "International Journal of Information Management Data Insights" 2021, vol. 1(2), **DOI: https://doi.org/10.1016/j.jjimei.2021.100013**.

Smith G.S., *Recognizing and Preparing Loss Estimates from Cyber-Attacks*, "Information Systems Security" 2004, vol. 12(6), **DOI: https://doi.org/10.1201/1086/44022.12.6.20040101/79786.8**.

Spasenic Z., Milosavljevic M., Milanovic N., *Project Financing of Renewable Energy Projects: A Bibliometric Analysis and Future Research Agenda*, "Fresenius Environmental Bulletin" 2022, vol. 31(8).

Trimborn S., Li M., Härdle W.K., *Investing with Cryptocurrencies – a Liquidity Constrained Investment Approach*, "Journal of Financial Econometrics" 2019, vol. 18(2), **DOI: https://doi.org/10.1093/jjfinec/nbz016**.

Turner A.B., McCombie S., Uhlmann A.J., *Discerning Payment Patterns in Bitcoin from Ransomware Attacks*, "Journal of Money Laundering Control" 2020, vol. 23(3), **DOI: https://doi.org/10.1108/jmlc-02-2020-0012**.

Wang X., An B., Chan H., *Who Should Pay the Cost: A Game-Theoretic Model for Government Subsidized Investments to Improve National Cybersecurity*, [in:] *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence*, 2019, **DOI: https://doi.org/10.24963/ijcai.2019/834**.

Williamson D.T., Staley A.B., *Ransomware: Tax Compliance Issues for a New Reality*, "Tax Management Memorandum" 2017, vol. 58(12).

Xi D., O'Brien T.I., Irannezhad E., *Investigating the Investment Behaviors in Cryptocurrency*, "Journal of Alternative Investments" 2020, vol. 23(2), **DOI: https://doi.org/10.3905/jai.2020.1.108**.

Young A.L., Yung M., *Cryptovirology*, "Communications of the ACM" 2017, vol. 60(7), **DOI: https://doi.org/10.1145/3097347**.

Yuryna Connolly A., Borrion H., *Reducing Ransomware Crime: Analysis of Victims' Payment Decisions*, "Computers and Security" 2022, vol. 119, **DOI: https://doi.org/10.1016/j.cose.2022.102760**.

Zimba A., Chishimba M., *On the Economic Impact of Crypto-Ransomware Attacks: The State of the Art on Enterprise Systems*, "European Journal for Security Research" 2019, vol. 4(1), **DOI: https://doi.org/10.1007/s41125-019-00039-8**.

Online sources

Claroty, *The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption*, 2021, https://security.claroty.com/report/global-state-industrial-cybersecurity-survey-2021 (access: 16.11.2022).

CoveWare, *Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022*, 28.7.2022, https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022 (access: 15.11.2022).

Donovan F., *CISOs Stockpile Cryptocurrency in Case of Ransomware Attack*, 25.7.2018, https://healthitsecurity.com/news/cisos-stockpile-cryptocurrency-in-case-of-ransomware-attack (access: 16.11.2022).

Elam E., Wange B., *Florida Follows North Carolina in Prohibiting State Agencies from Paying Ransoms*, 23.7.2022, https://www.databreaches.net/florida-follows-north-carolina-in-prohibiting-state-agencies-from-paying-ransoms (access: 16.11.2022).

European Union Agency for Cybersecurity, *ENISA Threat Landscape 2021*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (access: 27.10.2022).

Freed B., *North Carolina Moves Toward Ban on Ransomware Payments*, 14.5.2021, https://statescoop.com/north-carolina-moves-toward-ban-on-ransomware-payments (access: 16.11.2022).

International Accounting Standards Board, *Conceptual Framework 2018*, https://www.ifrs.org/projects/completed-projects/2018/conceptual-framework (access: 10.11.2022).

Labro T., *Ransomware, la nouvelle doctrine française*, 23.9.2022, https://paperjam.lu/article/ransomware-nouvelle-doctrine-f (access: 16.11.2022).

McKeith S., *Australia to Consider Banning Paying of Ransoms to Cyber Criminals*, 14.11.2022, https://www.reuters.com/technology/australia-consider-banning-paying-ransoms-cyber-criminals-2022-11-12 (access: 16.11.2022).

Pain D., Noordhoek D., *Ransomware: An Insurance Market Perspective*, July 2022, https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/ransomware_web.pdf (access: 15.11.2022).

Ransomware Task Force, *Combating Ransomware*, 2021, https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf (access: 16.11.2022).

Rasch M., *States Prohibit Ransomware Payments*, 8.7.2022. https://securityboulevard.com/2022/07/states-prohibit-ransomware-payments (access: 16.11.2022).

Rauch S., *The Rise of Ransomware in the Era of Covid-19*, 28.10.2021, https://www.simplilearn.com/rise-of-ransomware-in-the-era-of-covid-article (access: 16.11.2022).

Republic Geodetic Authority (RGZ), *IT infrastruktura RGZ meta intenzivnog hakerskog napada*, 15.6.2022, https://www.rgz.gov.rs/vesti/5028/vest/it-infrastruktura-rgz-a-meta-intenzivnog-hakerskog-napada (access: 15.11.2022).

Slattery T., Kirrane G., *How to Manage the Risk of a Ransomware Attack*, 20.5.2021, https://www.ey.com/en_ie/cybersecurity/how-to-manage-the-risk-of-a-ransomware-attack (access: 17.10.2022).

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, 21.9.2021, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf (access: 17.11.2022).

Legal acts

Conceptual Framework for Financial Reporting (consolidated text, 2018).

Criminal Code of the Republic of Serbia.

Law on Accounting and Auditing of the Republic of Serbia.

Law on Corporate Profit Tax of the Republic of Serbia.

Law on Digital Property of the Republic of Serbia.
Law on Information Security of the Republic of Serbia.
Law on Obligations of the Republic of Serbia.
Law on Personal Data Protection of the Republic of Serbia.
Law on Value Added Tax of the Republic of Serbia.
Rulebook on Chart of Accounts of the Republic of Serbia.
Rulebook on Value Added Tax of the Republic of Serbia.

ABSTRAKT

Oprogramowanie typu *ransomware* jest obecnie istotnym zagrożeniem w zakresie cyberbezpieczeństwa. W niniejszym artykule analizujemy finansowe konsekwencje ataków typu *ransomware*, a także motywy zapłaty okupu przez ofiarę takiego ataku oraz prawne, bilansowe i podatkowe konsekwencje takiej zapłaty. Podejście metodologiczne zastosowane w pracy stanowi połączenie metody formalno-dogmatycznej z metodą krytyki literatury. Na początku opisujemy wszelkie potencjalne straty, jakie mogą wynikać z ataku *ransomware*. Następnie poddajemy analizie warunki, w których zapłata przez jednostkę organizacyjną okupu jakiegokolwiek rodzaju, w tym wymuszonego drogą komputerową, jest legalna, a także inne względy, które ofiara musi wziąć pod uwagę, decydując się na zapłatę okupu. W tym zakresie analizujemy bilansowe i podatkowe implikacje strat poniesionych na skutek ataku *ransomware*, ze szczególnym uwzględnieniem zapłaty okupu.

Słowa kluczowe: ransomware; złośliwe oprogramowanie; płatność; konsekwencje bilansowe