Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 9, S. 122-128, 1, 2025

Araştırma Makalesi

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN:2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 9, pp. 122-128, 1, 2025

Research Article

Economic Impacts of Ransomware Attacks on the Slovak Cadastral Portal

František Vráb [*]

[1] *The Department of Economics and Management, University of Economics in Bratislava with seat in Košice, Slovakia*

[*]*(frantisek.vrab@euba.sk) Email of the corresponding author*

(Received: 18 January 2025, Accepted: 21 January 2025)

(2nd International Conference on Modern and Advanced Research ICMAR 2025, January 15-16, 2025)

ATIF/REFERENCE: Vráb, F. (2025). Economic Impacts of Ransomware Attacks on the Slovak Cadastral Portal. *International Journal of Advanced Natural Sciences and Engineering Researches*, 9(1), 122-128.

Abstract **–**This paper presents a comprehensive analysis of the ransomware attack on the Slovak Cadastral Portal in January 2025. We examine the attack's technical aspects, potential motives, and economic impacts, employing quantitative methods to assess the extent of the damage and the potential cascading effects on the Slovak economy. We also discussed the government's response options and the importance of robust cybersecurity measures for critical national infrastructure.

Keywords – Ransomware, Cyber Security, Critical Infrastructure, Economic Impact, Slovakia.

I. INTRODUCTION

The January 6, 2025, ransomware attack on the Slovak cadastral portal serves as a stark reminder of the growing threat environment facing modern organizations. This incident, which paralyzed a critical component of the public administration system in Slovakia, perfectly describes the complexity and far-reaching consequences of hybrid threats in the digital age. As outlined in the previous introduction, these threats transcend traditional boundaries and combine conventional attack vectors with sophisticated cyberwarfare tactics to destabilize and disrupt.

The attack on the cadastral portal, although ostensibly a straightforward ransomware incident, exemplifies the multifaceted nature of hybrid threats. By targeting a system vital to property transactions, banking operations and tax revenue collection, the attackers potentially sought not only financial gain, but also to sow discord and undermine public trust in government institutions. This convergence of criminal motives with potential geopolitical implications highlights the blurred lines of modern security challenges.

This contribution will focus on the specifics of the attack on the Cadastral Portal, analyze its technical aspects, potential motives and immediate and long-term economic consequences for Slovakia. By examining the government's response and the broader implications for national cyber security, we seek to draw valuable lessons for organizations grappling with the evolving threat of hybrid warfare. The cadastral crisis serves as a compelling case study that highlights the urgent need for robust cybersecurity measures, proactive threat identification, and comprehensive security management strategies to protect critical national infrastructure in an increasingly connected and volatile world.

II. MATERIALS AND METHOD

Describe in detail the materials and methods used when conducting the study. The citations you make from different sources must be given and referenced in references.

2.1 Data Collection

This study will use a combination of quantitative and qualitative data to analyse the economic impact of the ransomware attack on the Slovak Cadastral Portal. Quantitative data will be collected from publicly available sources, including government reports, statistical databases, and financial news outlets. This data will include:

- Slovakia's GDP growth rate and composition
- Real estate market data, including transaction volumes and prices
- Construction sector data, such as permits issued and project delays
- Government revenue data, including property tax collection
- Banking sector data, such as mortgage approvals and lending rates

Qualitative data will be collected through semi-structured interviews with key stakeholders, including government officials, business representatives, and industry experts. These interviews will provide insights into the operational and policy impacts of the attack, as well as potential long-term consequences for the Slovak economy.

2.2 Methodology

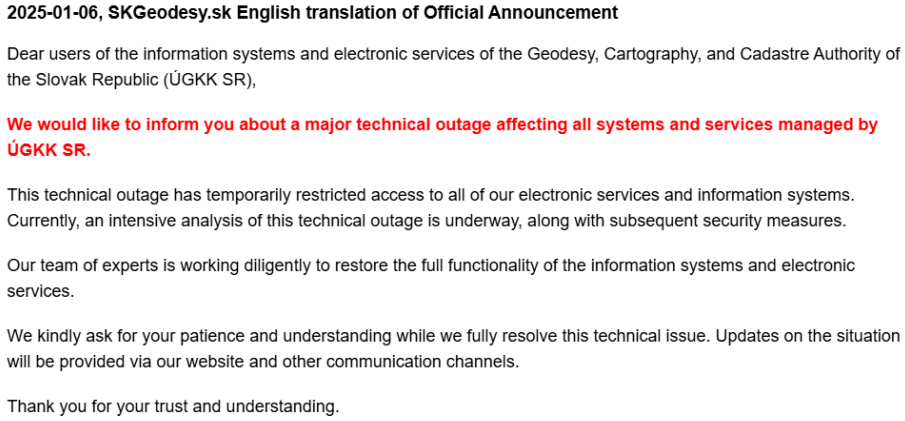
Quantitative data will be analysed using econometric techniques to assess the relationship between the Cadastral Portal's downtime and key economic indicators. Specifically, we will use time series analysis to compare economic performance before, during, and after the attack, controlling for other factors that may have influenced the observed changes.

We will also use input-output analysis to estimate the ripple effects of the attack on various sectors of the Slovak economy. This method allows us to trace how disruptions in one sector, such as real estate or construction, can spread to other interconnected industries

Qualitative data from interviews will be analysed using thematic analysis to identify key themes and patterns in stakeholder perceptions and experiences. This will involve coding interview transcripts to identify recurring topics and relationships between them. The results of the qualitative analysis will complement the quantitative findings by providing context and insights into the nuanced impacts of the attack.

2.3 Limitations

This study is subject to several limitations. First, the availability of timely and detailed data may be limited, particularly for certain economic sectors or qualitative aspects of the attack's impact. Second, the complexity of the economic system makes it difficult to isolate the specific effects of the Cadastral Portal's downtime from other factors that may have influenced economic performance during the same period. Finally, the study's reliance on stakeholder interviews may introduce some subjectivity into the analysis, although efforts will be made to ensure the diversity and representativeness of interviewees.



2025-01-06, SKGeodesy.sk English translation of Official Announcement

Dear users of the information systems and electronic services of the Geodesy, Cartography, and Cadastre Authority of the Slovak Republic (ÚGKK SR),

We would like to inform you about a major technical outage affecting all systems and services managed by ÚGKK SR.

This technical outage has temporarily restricted access to all of our electronic services and information systems. Currently, an intensive analysis of this technical outage is underway, along with subsequent security measures.

Our team of experts is working diligently to restore the full functionality of the information systems and electronic services.

We kindly ask for your patience and understanding while we fully resolve this technical issue. Updates on the situation will be provided via our website and other communication channels.

Thank you for your trust and understanding.

Fig. 1 Slovak original announcement

Figure 1 shows the official notification of the Office of Geodesy, Cartography and Cadastre of the Slovak Republic, which informs users about a major technical outage of all their systems and services. The outage limited access to all electronic services and information systems.

III. RESULTS

Results should be clear and concise. The most important features and trends in the results should be described but should not interpreted in detail.

3.1 Short-term Impacts (Up to 1 Week)

Minimal impact on property transactions: While there may be some delays in processing transactions, the overall impact on the real estate market is expected to be limited.

Minor inconvenience to businesses and citizens: Individuals and businesses may experience some inconvenience due to the unavailability of the portal, but the impact on their daily operations is likely to be minimal.

3.2 Medium-term Impacts (1 Week to 1 Month)

Significant impact on the real estate sector: The inability to register property transactions and verify ownership could significantly disrupt the real estate market, leading to delays in sales, construction projects, and mortgage approvals.

Construction sector slowdown: The construction sector may experience delays due to the inability to obtain necessary permits and register properties.

Impact on the banking sector: Banks may face difficulties processing mortgage applications and securing property collateral, potentially leading to a slowdown in lending.

Reduced tax revenue: The government may experience a decline in property tax revenue due to the inability to process registrations and assess property values.

3.3 Long-term Impacts (Exceeding 1 Month)

Critical economic disruption: A prolonged shutdown of the portal could have severe economic consequences, as it would hinder the functioning of various sectors and disrupt financial flows.

Cascading effects on the economy: The economic impact could extend beyond the real estate, construction, and banking sectors, affecting other industries that rely on property transactions and related services.

Loss of public trust: A prolonged crisis could erode public trust in the government's ability to protect critical infrastructure and maintain essential services, potentially leading to economic uncertainty and reduced investment.

3.4 Quantitative Analysis

This section aims to quantify the potential economic repercussions of a disruption to the Cadaster portal in Slovakia. Given the portal's crucial role in property transactions, construction permitting, and land administration, its unavailability can have cascading effects across multiple sectors. To assess these impacts, we employ the following data and assumptions:

Data and Assumptions

- *Slovakia's GDP in 2023:* Approximately 132 € billion [6]
- *Real Estate Market Value:* Estimated at 500 € billion [7]
- *Construction Sector Contribution to GDP*: 6.5% [5]
- *Property Tax Revenue:* 800 € million annually [5]
- *Average daily property transactions:* 500 [5]
- *Average value of property transactions*: 200,000 € [5]

We will analyse potential economic losses under different disruption scenarios, considering varying durations and degrees of service impairment.

Scenario 1: Complete Outage for One Day

Direct Impacts:

- *Lost Transaction Value:* 500 transactions * 200,000/transaction = 100 € million
- *Lost Property Tax Revenue:* (800 million/year) / 365 days = 2.19 € million

Indirect Impacts:

- *Construction Delays:* Assuming a 1-day delay in 50% of ongoing construction projects due to permit issues, with an average daily project value of €1 million, the impact would be 0.5 * 1 € million * number of affected projects. This number needs to be sourced from construction sector data.
- *Reduced Productivity:* Disruption in land administration processes can affect various sectors, including legal, financial, and real estate. Estimating productivity losses requires further research and data on the number of employees and businesses reliant on the Cadastre portal.

Overall Impact:

- The total economic loss for a one-day outage can be estimated by summing the direct and indirect impacts. This can be further refined by incorporating GDP contribution data for affected sectors.

Scenario 2: Partial Outage for Multiple Days

This scenario involves limited functionality of the Cadastre portal for an extended period. The economic impact will depend on the specific services affected and the duration of the disruption. For example, if online property searches are unavailable, it could significantly slow down real estate transactions and related activities.

Scenario 3: Targeted Attack on Specific Services

A targeted attack could disrupt specific functionalities, such as access to land ownership records or the submission of online applications. The economic impact will vary depending on the targeted service and its importance to different user groups.

GDP Impact Analysis

To estimate the impact on GDP, we can use the following approach:

1. *Identify Affected Sectors*: Determine the sectors directly and indirectly affected by the Cadaster portal disruption (e.g., real estate, construction, legal, financial).
2. *Estimate Sectoral Output Loss:* Quantify the decrease in output for each affected sector based on the disruption scenarios.
3. *Calculate GDP Impact:* Multiply the sectoral output loss by the sector's contribution to GDP.

For instance, if the construction sector experiences a 10% output loss due to a Cadastre portal outage, and the sector contributes 6.5% to GDP, the estimated GDP impact would be 0.10 * 0.065 * 132€ billion = 858 € million.

Limitations and Future Research

This analysis provides a preliminary estimate of the potential economic losses. More accurate quantification requires further research and data collection, including:

- Detailed data on the volume and value of transactions processed by the Cadastre portal.
- Surveys to assess the impact of portal disruptions on businesses and individuals.
- Development of economic models to capture the complex interdependencies between the Cadastre portal and various economic sectors.

By conducting a comprehensive analysis and refining the data inputs, we can gain a more precise understanding of the economic consequences associated with Cadastre portal disruptions and inform strategies for mitigating these risks.

IV. DISCUSSION

The ransomware attack on the Slovak Cadastral Portal in January 2025 served as a stark wake-up call, exposing critical vulnerabilities in Slovakia's national infrastructure and its susceptibility to significant economic disruption. By completely shutting down the portal, the attack disrupted property transactions, hindered banking operations, and impacted state tax revenue collection. This incident highlighted the interconnectedness of digital systems and the far-reaching consequences of cyberattacks on essential services.

Economic and Societal Impact: The economic fallout from the attack was potentially immense, with estimated losses reaching billions of euros, contingent on the duration of the portal's downtime. The real estate, construction, and banking sectors bore the brunt of the disruption. Property transactions faced delays, mortgage approvals were stalled, and construction projects were potentially jeopardized, leading to uncertainty and financial repercussions for businesses and individuals alike. Beyond the immediate economic impact, the attack eroded public trust in digital services and raised concerns about the security of personal data.

Response and Recovery: The Slovak government responded swiftly by mobilizing IT professionals to restore the system and bolster security measures. This reactive approach, while necessary, underscored the need for proactive risk management and a comprehensive cybersecurity strategy. International cooperation emerged as a crucial element in combating cyber threats, facilitating the sharing of intelligence, best practices, and resources.

Legal and Ethical Considerations: The attack raised critical legal and ethical questions surrounding data protection, cybercrime legislation, and government accountability. Ensuring the protection of citizens' data, upholding ethical principles in the digital realm, and establishing clear lines of responsibility in the event of cyberattacks are paramount. Addressing these issues transparently and proactively will foster trust and accountability.

Strengthening Cybersecurity Posture: This incident provided a valuable opportunity for Slovakia to learn from international best practices and enhance its cybersecurity preparedness and resilience. By strengthening its national cybersecurity framework, investing in critical infrastructure protection, and fostering public-private partnerships, Slovakia can bolster its defences against future cyber threats. Promoting cybersecurity awareness among citizens and businesses is equally important in creating a collective defence against cybercrime.

Call for Comprehensive Action: The ransomware attack on the Slovak Cadastral Portal serves as a potent reminder of the escalating threat of cyberattacks to critical infrastructure globally. It underscores the necessity of a comprehensive approach to cybersecurity, encompassing technological solutions, human factors, and international collaboration. By investing in cybersecurity, promoting awareness, and collaborating with international partners, Slovakia can fortify its resilience against future cyber threats, safeguarding its critical infrastructure, economic stability, and digital society.

Fig. 2 Key elements of organizational security management

Figure 1 illustrates the key elements of an organization's security management and presents them as interconnected parts of a complex system. At the heart of the diagram is "Organizational Security Management," which emphasizes its central role in protecting an organization's assets. Surrounding this core are nine key elements, each representing a circle. [4]

Organizational Security Management: The attack highlighted the critical importance of robust organizational security management within all government agencies and businesses. This encompasses a range of activities and processes designed to protect an organization's assets, including:

- *Risk Management:* Identifying, assessing, and mitigating potential threats.
- *Information Protection:* Implementing measures to safeguard sensitive data.
- *Physical Security:* Protecting physical assets and infrastructure.
- *Business Continuity Planning:* Ensuring operational continuity in the event of disruptions.
- *Training and safety awareness:* Running campaigns to raise awareness of risks and best practices.
- *Incident Management:* Analysing of the causes of incidents and development plans.
- *Compliance with regulations and standards:* Analysing network and detect threats.
- *Audit and evaluation:* Assessing the effectiveness of the security system

Effective organizational security management requires an integrated approach that involves all employees and stakeholders. It is crucial to establish clear security policies, provide regular training, and foster a culture of security awareness.

By adopting a comprehensive and proactive approach to cybersecurity, Slovakia can learn from this incident and emerge stronger and more resilient in the face of future cyber threats.

V. CONCLUSION

This study has highlighted the critical importance of the Cadastre portal to the Slovak economy. The portal facilitates a wide range of essential transactions, impacting property sales, construction projects, and overall economic activity. A disruption to the portal's functionality would have significant consequences, hindering these processes and potentially leading to substantial financial losses.

Based on Slovakia's 2023 GDP, it is estimated that a complete non-functionality of the Cadastre portal could result in damages exceeding 3 million euros per day. Even a 1% decrease in daily GDP due to portal outage translates to approximately 3,347,940 euros (or 3,616,403 USD) per day. This figure, a conservative estimate, underscores the portal's vital role in maintaining economic stability and growth.

The findings of this study emphasize the need for robust measures to ensure the continuous and reliable operation of the Cadastre portal. Investing in preventative maintenance, cybersecurity, and disaster recovery plans is crucial to minimize the risk of disruptions and mitigate potential economic damage.

ACKNOWLEDGMENT

The author expresses his sincere thanks to the company Training & Consulting, s.r.o., for its invaluable contribution to this research effort. Their unwavering commitment to solving complex organizational challenges, together with their generous support, insight and expertise, were key to the successful completion of this study. We also thank the cyber security community, which is taken care of by the National Coordination Canter of the Slovak Republic (NCC-SK). Their commitment to enhancing national cybersecurity capabilities and fostering collaboration has created a supportive environment for research and innovation in this critical area.

REFERENCES

[1] Bartoš, Alexander. 2022. The fog of hybrid warfare. Another view of the conflicts of the 21st century.2022. Torden.
[2] Gombár, M. Vagaská, A. Korauš A. Račková, P. Pavlína. Application of Structural Equation Modelling to Cybersecurity Risk Analysis in the Era of Industry 4.0. Journal of Cybersecurity, 2023, roč. 5, č. 2, s. 120-135.
[3] Ministry of the Interior of the Slovak Republic. 2024.Press release on bomb threats. https://tinyurl.com/y2tmweny
[4] Nowicka, J., Ciekanowski, Z., Czternastek, M., Król, A., & Kacprzak, M. (2024). Navigating Hybrid Threats: Advanced Security Solutions for Modern Organizations. European Research Studies Journal, 27(2), 488-499.
[5] https://economy-finance.ec.europa.eu/document/download/e2c1dea3-1062-4824-a06d-4219d1e31f9b_en?filename=SWD_2024_625_1_EN_Slovakia.pdf
[6] https://tradingeconomics.com/slovakia/gdp
[7] https://tradingeconomics.com/slovakia/gdp-from-construction
[8] Vráb, František. 2023. A model for the prevention of hybrid threats in the enterprise environment. In: MTP no. 2, s. 32-38. https://tinyurl.com/3vv27wb3
[9] Vráb, F. (2023). Hybrid threats in the context of bombings to schools: multidisciplinary analysis and proposals for Slovakia in a global context. In MTP no.