SECTION 1. THE WAR'S GEO-ECONOMIC CONSEQUENCES AND THE TRANSFORMATION OF INTERNATIONAL ECONOMIC RELATIONS

DOI https://doi.org/10.30525/978-9934-26-613-3-1

THEORETICAL BACKGROUND OF CYBER THREATS TO MUNICIPALITIES IN THE SLOVAK REPUBLIC

ГЕОЕКОНОМІЧНІ НАСЛІДКИ ВІЙНИ ТА ТРАНСФОРМАЦІЯ МІЖНАРОДНИХ ЕКОНОМІЧНИХ ВІДНОСИН

Adamko J.
Ing. MSc., MBA.,
PhD at the Department of Social Sciences
Institute of Technology and Economics in Prešov
Prešov, Slovakia

1 Cyber attacks

Cyber attacks have become a global threat that affects not only large international corporations or state institutions, but also smaller entities such as municipalities and districts. In the digital age, where many local governments depend on information technology and online services, cyber incidents can paralyze their daily functioning and have devastating consequences for the lives of residents.

Municipalities and districts often manage critical infrastructure, from energy and water supplies to healthcare systems, educational institutions and transport. In addition, they are responsible for managing sensitive data of residents, such as personal information, financial data and property records. One of the main factors why municipalities and districts are vulnerable is insufficient security.

Historical development of cyber threats

With the advent of the Internet in the 1990s, cyber threats began to escalate. Computer viruses and worms, such as Melissa (1999) and ILOVEYOU (2000), spread through email and affected millions of devices worldwide. These attacks caused widespread damage and demonstrated that computers are extremely vulnerable to the spread of malware. [1, p. 45]

Modern attacks use social engineering techniques such as phishing and malware that spreads through vulnerabilities in software systems.

There is also a trend towards the rise of **Distributed Denial of Service** (DDoS) attacks, which overload servers and network resources, leading to service outages. [2, p. 3].

1.1 Cyberattacks can have far-reaching consequences for municipalities and districts:

Financial losses – not only direct ransom payments in the case of ransomware attacks, but also the costs of restoring systems, investigating and implementing better security measures can pose a great burden for municipalities. In addition, loss of data or interruption of services can lead to a decrease in public trust, which can indirectly translate into further losses.

Paralysis of critical services – infrastructure such as public transport, water and electricity distribution can be temporarily paralyzed, which has a direct impact on the lives of residents.

Loss of public trust – citizens expect their personal data to be safe.

Legal consequences – in the context of data protection laws such as the European GDPR, municipalities can be fined for insufficient data security.

The consequences of cyber attacks can be extensive, from financial losses, disruption of operations to reputational damage. According to studies, losses caused by cyber attacks reach billions of dollars globally per year. In the case of successful attacks, there is a disruption of service provision, theft of personal data and sensitive information, which can lead to legal consequences due to violations of regulations such as the GDPR. In addition, the consequences of attacks can be a loss of trust from customers, which has an indirect economic impact on businesses and organizations. [3, p. 3]

Types of cyber attacks include various forms of intrusion that attackers use to exploit vulnerabilities in systems.

Ransomware is a specific form of malicious software (malware) that aims to encrypt a victim's data and then demand a ransom for its decryption. [4, p.17]

Phishing je forma kybernetického útoku založená na sociálnom inžinierstve, pri ktorom útočníci predstierajú, že sú dôveryhodná inštitúcia alebo osoba, aby podvodom získali citlivé informácie, ako sú heslá, finančné údaje či osobné údaje. [5, p .20]

DDoS (Distributed Denial of Service) útoky predstavujú formu kybernetického útoku, pri ktorom útočníci preťažia cieľový server, sieť alebo službu veľkým množstvom simultánnych požiadaviek, čím spôsobia jeho dočasnú nedostupnosť pre legitímnych používateľov. [6, p.145]

1.1.1 Cyberattacks and their impact on municipalities and districts

Cyberattacks represent serious and sophisticated threats aimed at damaging, disrupting or unauthorized access to computer systems, networks, software or data. The basis of a cyberattack is an intentional activity carried out by an individual or organization with the aim of gaining unauthorized

benefits or harming a target entity. These attacks exploit technology vulnerabilities, user errors or insufficiently implemented security measures.

Cyberattacks can have far-reaching consequences for municipalities and districts, such as:

Financial losses – not only direct ransom in the case of ransomware attacks, but also the costs of restoring systems, investigating and implementing better security measures can pose a great burden for municipalities.

Paralysis of critical services – infrastructure such as public transport, water and electricity distribution can be temporarily paralyzed, which has a direct impact on the lives of residents.

Loss of public trust – citizens expect their personal data to be secure.

Legal consequences – under data protection laws such as the European GDPR, municipalities can be fined for insufficient data security. [7, p. 146]

1.1.2 The importance of protecting against cyberattacks

Cyberattacks represent one of the most significant threats in the modern digital world, and it is therefore essential that organizations and individuals implement effective security measures to protect their systems and data. Protection against these attacks is crucial to maintaining the trust of customers, partners and the public. The essential elements of protection are antivirus programs, firewalls, encryption and regular data backups, which minimize the risk of sensitive data being compromised or lost.

1.3 Cyber Insurance as a Risk Spreading Tool

Cyber insurance has become an important tool in recent years to mitigate the risks associated with cyber attacks. This type of insurance offers protection against various types of cyber threats, such as ransomware attacks, data breaches and business interruptions caused by attacks. For local governments that manage sensitive data and critical services, cyber insurance is a key means of covering the financial costs that could result from attacks.

Cyber insurance is a type of commercial insurance designed to cover losses resulting from cyber incidents and attacks, such as data breaches, theft of personal information, destruction of systems or business interruption due to attacks. These policies provide coverage for various costs, such as system recovery costs, legal fees, liability for personal data breaches and the costs of communicating with affected individuals.

Cyber insurance helps cities and municipalities compensate for these losses and allows them to recover from incidents more quickly. [8, p,19]

1.3.1 Types of Cyber Insurance

The most important types of cyber insurance include insurance against ransomware attacks, data breaches and DDoS (Distributed Denial of Service) attacks. Each of these types provides specific coverage depending on the type of cyber threat, with the aim of reducing the financial and operational consequences of attacks on organizations and institutions.

Ransomware is one of the most common and dangerous types of cyber attacks, in which attackers encrypt the victim's data and demand a ransom to restore it. Ransomware insurance is designed to cover the costs associated with the attack, including the ransom (if the organization chooses to pay it), the costs of data recovery, legal fees, and other costs to mitigate the damage. These policies may also include the costs of investigating the incident and communicating with affected parties. [9, p.4]

Data Breach Insurance

Data breach is another common problem faced by many organizations. This type of insurance covers the costs associated with the leakage of sensitive data, such as personal information about customers, employees, or financial data. Data breach insurance includes the costs of data recovery, notification of affected parties, legal costs, as well as reputational costs associated with the leakage of sensitive data. [10, p.17]

DDoS Insurance

DDoS insurance provides coverage for the costs associated with downtime, system recovery, and the costs associated with dealing with an attack. This insurance is important for organizations that rely heavily on the continuous operation of their online services. The costs associated with downtime can be very high, especially for e-commerce companies, financial institutions, or government organizations that provide critical services. [11, p. 22]

2 Current Status of Cyber Security in Municipalities and District In Slovakia

The need to increase cybersecurity in municipalities is mainly based on legislative requirements. The requirements for the level of IT security in municipalities are based on Act No. 69/2018 Coll. on Cyber Security. The need to increase the security of public administration IT systems is stated in the NBU report on cybersecurity in 2023, according to which an increase in the number of security incidents is recorded.

The involvement of currently unconnected municipalities in the IS DCOM is to cost 2.3 million euros, increasing the number of connected municipalities should be part of a separate project. The involvement of municipalities in the IT system DCOM is voluntary, municipalities can solve the provision of electronic services independently or purchase solutions from commercial entities. The migration of 350 municipalities with a cost of 2.3 million euros should therefore not be part of the project to increase cybersecurity. [12, p. 23]

The creation of security procedures for municipalities is expected to cost a total of 4.8 million euros, the cost per municipality is 2.6 thousand euros. According to contracts available in the Central Register of Contracts (CRZ), municipalities procure cybersecurity services for 18-72 euros per month, the costs include the creation of documentation and support in resolving incidents. [13, p. 24]

2.1 Identification of the research problem

Cyber attacks represent an ever-growing threat to municipalities and districts that manage critical infrastructure and sensitive data of their citizens. A significant factor contributing to this vulnerability is the lack of financial resources to implement advanced security solutions and for continuous training of employees, which leads to a more frequent occurrence of successful attacks.

Cyber attack insurance can cover the costs of system restoration, legal liabilities and ransom payments, but the process of obtaining this insurance is often complex and expensive.

The research problem is therefore the question of the extent to which cyber insurance can effectively mitigate the financial and operational consequences of cyber attacks in local governments, and what are the best strategies to improve its effectiveness. This research will include an analysis of current insurance products, an assessment of criteria for obtaining insurance, a study of real cases of successful and unsuccessful use of cyber insurance, as well as the identification of optimal practices for improving cybersecurity in municipalities and districts.

Characteristics of the research sample

The research sample consisted of 120 municipalities in Slovakia, which were selected based on the following criteria to ensure representativeness and diversity in the research on cyber attacks and insurance. In total, we addressed 270 municipalities.

Table 1

Characteristics of the sample of respondents: size of the municipality, geographical location, economic profile and budget of the municipalities

Municipality size	Number	% representation in the sample
Small municipalities (up to 2000 inhabitants)	40	33,3 %
Medium-sized (2001 – 10,000 inhabitants municipalities) Large municipalities (over 10,000 inhabitants)	40 40	33,3 % 33,3%

Source: own processing /based on survey/

This aspect will ensure that municipalities with different financial possibilities are included, which is key to understanding how financial resources affect the ability of municipalities to implement security measures and obtain cyber insurance.

For semi-structured interviews, the sample of research respondents was ten randomly selected mayors and IT specialists with the following survey questions and hypotheses:

1. What are the most common types of cyber attacks in Slovak municipalities and districts?
2. What measures are currently in place to protect against cyber attacks?
3. What is the impact of cyber attacks on financial losses and operational processes of municipalities and districts?
4. What insurance products are available on the Slovak market to cover cyber risks and what is the scope of their coverage?
5. How effective are current measures and insurance products in mitigating the impacts of cyber attacks?
6. What are the main obstacles to taking out cyber risk insurance in municipalities and districts?
7. What specific steps and measures should be implemented to improve cybersecurity and effectively use insurance?

Hypotheses

Hypothesis H1: The introduction of cyber insurance significantly reduces financial losses of municipalities and districts after cyber attacks.

Hypothesis H2: Local governments with a higher level of implementation of security measures achieve better cyber insurance conditions.

Hypothesis H3: Training employees to recognize cyber threats reduces the frequency of successful cyber attacks on local governments.

Hypothesis H4: Insurance against cyber attacks supports faster recovery and restoration of operations of local governments after an incident.

Hypothesis H5: Municipalities and districts that have comprehensive security policies and procedures in place report lower overall costs of cyber incidents in the long term.

Survey methods were used and we use a combination of quantitative and qualitative research methods to obtain detailed and relevant data on the current state of cybersecurity in Slovak municipalities and districts.

The questionnaire was designed based on a thorough literature review and existing studies in the field of cybersecurity and insurance. The questions in the questionnaire are aimed at identifying the most common types of cyber attacks, existing security measures and policies in municipalities, the level of awareness and training of employees, experiences with cyber attacks and their impact, as well as the use of cyber insurance and the conditions for obtaining it.

The questionnaire contains a combination of closed questions with answer options that allow for quantitative analysis, Likert scales to measure the

degree of agreement or frequency, and open-ended questions that provide space for more detailed answers and obtaining qualitative data. Before distribution, the questionnaire was pilot-tested on a small sample of five municipalities to verify the clarity and relevance of the questions. Based on feedback from pilot respondents, necessary adjustments to the questionnaire were made.

The questionnaires were distributed electronically via an online platform (Google Forms). Respondents were contacted via the official email addresses of the municipalities or by telephone, and were given a time frame of two to three weeks to complete the questionnaire.

Semi-structured interviews

The second phase of data collection consisted of semi-structured interviews with representatives of municipalities and insurance companies. The aim of these interviews was to gain a deeper understanding of the challenges and opportunities in the field of cybersecurity and insurance. Interviewees were selected based on interesting or significant responses in the questionnaire, and we reached approximately 15 to 20 respondents (10 representatives of municipalities and 5 representatives of insurance companies).

The interviews were conducted through personal meetings, telephone calls, or video conferences, depending on the preferences of the participants and current possibilities. Each interview lasted approximately 45 to 60 minutes.

Secondary data analysis

The third data source is the analysis of secondary data from publicly available sources and databases. The sources include official reports and statistics from the National Security Office of the Slovak Republic, the Ministry of the Interior of the Slovak Republic, the Slovak Insurance Association, as well as professional literature, books, scientific articles and conference papers related to cybersecurity and insurance. We also used online sources such as websites of professional organizations and current reports on cyber incidents.

Data processing and comparison

We used a combination of quantitative and qualitative methods to process and analyze the obtained data. Quantitative data from the questionnaires were processed using statistical software, SPSS and Microsoft Excel. We performed descriptive statistics to calculate frequencies, means and standard deviations, as well as inferential statistics to test hypotheses using correlation analyses and statistical verification.

Survey quality assurance

To ensure the quality of the research, we conducted pilot testing of instruments such as the questionnaire and interview protocol to verify their comprehensibility and relevance. We used data triangulation by combining

different methods and data sources to verify the consistency of the findings. During the research, we consulted with experts and a trainer for continuous control of the research procedure, which contributed to increasing the validity and reliability of the survey.

3 Interpretation of Survey Results

How we defined the characteristics of the survey sample of 120 municipalities in Slovakia, which were selected based on the presented criteria to ensure representativeness and diversity in the survey on cyber attacks and insurance. In total, we addressed 270 municipalities, but only 120 municipalities were willing to participate, and the return rate of the questionnaires was only 44.44%. Despite the low return rate, we managed to ensure a sufficiently consistent research sample. It was a controlled selection, where we first contacted the representatives of the municipality by phone and later sent them the questionnaire by email. 4 municipalities refused to send the questionnaire by email for technical reasons, but were willing to participate in the research by filling out the paper form of the questionnaire. The municipalities were contacted randomly, according to a list of telephone and email contacts that we obtained from the Ministry of the Interior based on a request under Act 211/2000 on free access to information, until we managed to obtain a sufficiently large and consistent sample for the research. We then divided the sample according to these variables.

Based on the presented results of the questionnaire survey, the results achieved in the established hypotheses were verified.

Comparison of questionnaire surveys

Questionnaire question No. 1 Has your municipality/district encountered a cyber attack in the last 12 months?

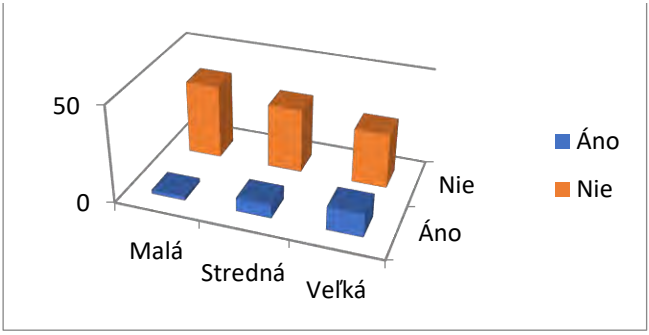

Fig. 1. Respondents' answers to question No. 1 by municipality size
Source: Own processing

The figure shows data on cyber attacks in municipalities divided by size (small, medium, large) over the last 12 months. It shows that smaller municipalities experience cyber attacks less frequently, while larger municipalities experience them more frequently.

Questionnaire question no. 2 by geographical location

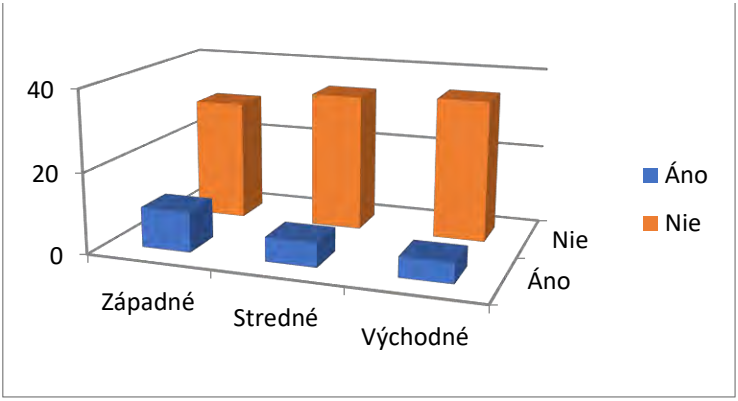

Fig. 2. Respondents' answers to question no. 1 by geographical location
Source: Own processing

The differences between regions are interesting, especially when we consider the potential causes of differences in experiences with cyber threats. In Western Slovakia, up to 25% of respondents reported (10 out of 40) that they have encountered a cyber attack. This higher share may indicate that the west of Slovakia, where there is a higher concentration of population, business activities and digitalized infrastructure, is a more attractive target for cyber attacks.

This result points to the need to increase awareness and strengthen preventive measures in the field of cybersecurity, especially in the west, where the incidence of attacks is higher.

Respondents' answers to question 1 by budget

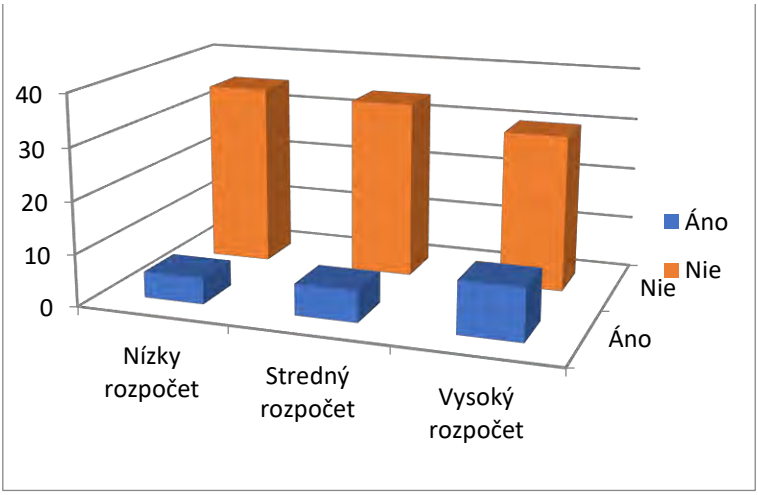

Fig. 3. Respondents' answers to question 1 by budget
Source: Own processing /by budget/

Over the past 12 months, 12.5% of municipalities with a low budget, 15% of municipalities with a medium budget and up to 25% of municipalities with a high budget have experienced cyber attacks. This trend suggests that higher budgets are associated with a greater likelihood of cyber attacks. This is probably related to a more extensive digital infrastructure and higher visibility, which makes these municipalities more attractive targets for attackers. Larger municipalities often manage more complex IT systems, which may contain more vulnerabilities and are therefore more susceptible to attacks.

Effective preventive measures are key to minimizing risks and ensuring the continuity of public services in the digital era.

Calculating the Chi-square statistic (χ^2)

- Low budget, Yes ≈0.571
- Low budget, No ≈0.121
- Medium budget, Yes ≈0.143
- Medium budget, No ≈0.030
- High budget, Yes ≈1.286
- High budget, No ≈0.273

Total χ^2: 0.571+0.121+0.143+0.030+1.286+0.273≈2.4040.571 + 0.121 + 0.143 + 0.030 + 1.286 + 0.273≈ 2.4040.571+0.121+0.143+0.030+1.286+0.273≈2.404

Determining the degrees of freedom (df)

df=(r−1)×(k−1)=(3−1)×(2−1)=2df = (r-1) (k-1) = (3-1) (2-1) = 2df=(r−1)×(k−1)=(3−1)×(2−1)=2

Determining the p-value

For $\chi^2 = 2.404$ and df = 2, the p-value is approximately 0.298.

Interpretation of the results

The p-value (0.298) is higher than the commonly used significance level ($\alpha = 0.05$). There is no statistically significant relationship between the budget of municipalities/districts and the incidence of cyberattacks. Although higher budgets have a higher number of attacks, this difference is not significant enough to reject the null hypothesis of independence. **The standard deviation (≈ 0.38)** shows how the responses are dispersed around the mean. In this case, the dispersion is relatively low, indicating that most municipalities answered consistently (mostly "No").

Standard deviations by budget categories

o Low budget ≈ 0.33

o Medium budget ≈ 0.36

o High budget ≈ 0.43

A higher SD value means a greater dispersion of responses. In this case, a higher SD for a high budget indicates a greater variability of responses (a greater number of "Yes" compared to other categories).

Question No. 2 If yes, what type of attack was it? (multiple choices possible

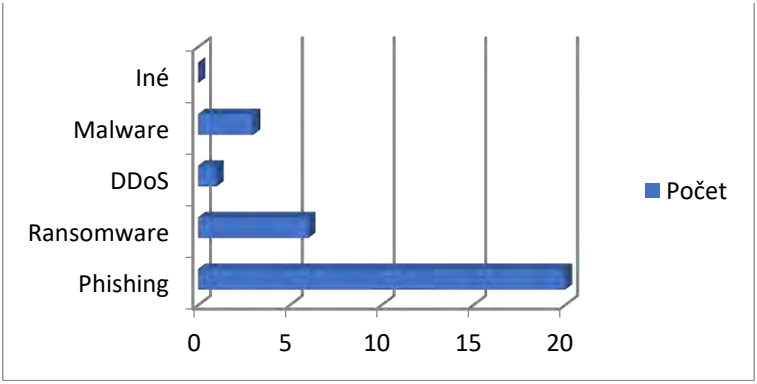

Fig. 4. Respondents' answers to question No. 2 by type of attack

Source: Own processing /by type of attack/

When analyzing question No. 2, it was found that out of the 21 municipalities that recorded a cyber attack, there were a total of 30 answers per type of attack, which means an average of 1.43 types of attacks per respondent. The most common type of attack was Phishing with 20 answers (66.67%), which indicates that attackers prefer social engineering to obtain sensitive information. This was followed by Ransomware with 6 answers (20%) and Malware with 3 answers (10%), which pose serious threats to the security and functioning of municipalities. DDoS attacks were relatively rare, recorded in only 1 case (3.33%), and no one reported other types of attacks. This distribution highlights the dominance of phishing, while ransomware and malware remain significant but less frequent threats. The average number of attacks suggests that some attackers are using a combination of methods to increase the success of their attacks.

Question No. 3 How many attacks have you experienced in the last 12 months? (specify the number)

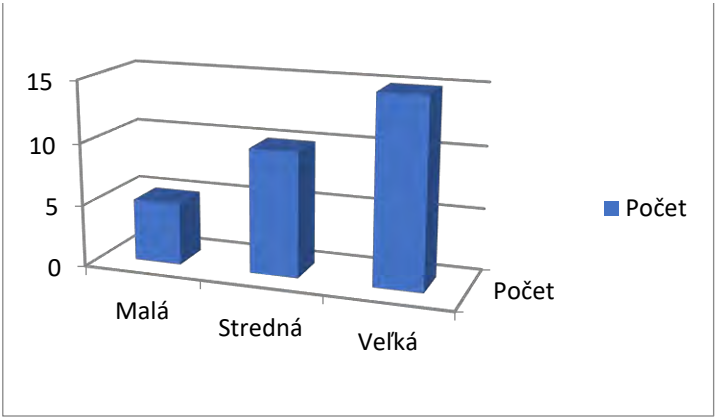

Fig. 3. Shows the number of recorded cyber attacks in the last 12 months by the size of the municipality

Source: Own processing /according to recorded cyber attacks/

Small municipalities experienced 5 attacks (16.67%), medium-sized municipalities experienced 10 attacks (33.33%) and large municipalities experienced 15 attacks (50%). This trend shows that large municipalities are most affected by cyber attacks, which may be a consequence of a more extensive digital infrastructure, higher visibility and a greater number of services provided, which make these municipalities more attractive targets for attackers.

Fig. 4. Shows the number of recorded cyber attacks in the last 12 months divided by regions of Slovakia

Western Slovakia with 13 attacks (43.33%), Eastern Slovakia with 10 attacks (33.33%) and Central Slovakia with 7 attacks (23.33%). This distribution indicates that the most attacks were recorded in Western Slovakia, which may be due to the higher concentration of digital services, larger infrastructure and attractiveness for attackers in this region. Eastern Slovakia recorded a medium number of attacks, while Central Slovakia is the least affected. The higher number of attacks in the Western region points to the need to prioritize robust cybersecurity measures in this area.

Descriptive statistics

Frequency and percentage

o Large municipality: 15 attacks (50.00%)

o Medium municipality: 10 attacks (33.33%)

o Small municipality: 5 attacks (16.67%)

Mean number of attacks

Standard deviation (SD)

$$\text{Rozptyl} = \frac{\sum(x_i - \bar{x})^2}{N} = \frac{(5 - 1.43)^2 + (10 - 1.43)^2 + (15 - 1.43)^2}{21} \approx 22.53$$

$$SD = \sqrt{22.53} \approx 4.75 \text{ útokov}$$

Inferential statistics

Selected statistical test: Poisson regression and Chi-square

The reason for choosing this statistical method is that the number of attacks is a type of count data that often follows a Poisson distribution. Poisson regression is suitable for modeling the relationship between the number of events and one or more independent variables (in this case, the size of the municipality).

Calculation procedure

1. Modeling

o Dependent variable: number of attacks (0, 1, 2, ...)

o Independent variable: size of the municipality (small, medium, large)

2. Model formulation:

Large municipalities have a statistically significantly higher number of attacks (p = 0.01) compared to small municipalities. Medium municipalities did not show a significant difference (p = 0.15) in the number of attacks compared to small municipalities.

Determining degrees of freedom (df)

df=(r−1)×(k−1)=(3−1)×(2−1)=2df = (r – 1) \ (k – 1) = (3 – 1) \ (2 – 1) = 2df=(r−1)×(k−1)=(3−1)×(2−1)=2

Comparison with the critical value

• For df = 2 and α = 0.05, the critical value is 5.991.

• If χ2>5.991χ² > 5.991χ2>5.991, we reject the null hypothesis.

$\chi^2 = 1.33 < 5.991 \rightarrow$ We do not reject the null hypothesis (H_0).

There is no statistically significant relationship between the size of the municipality and the number of recorded attacks. The distribution of attacks is approximately equal between the sizes of the municipalities.

Hypothesis testing

Hypothesis H1: The introduction of cyber insurance significantly reduces the financial losses of municipalities and districts after cyber attacks.

The interviews show that insurance can significantly help in mitigating the financial impacts of cyber attacks. Jana (profile 9) stated that insurance provided financial support in covering the costs of restoring systems and minimizing the impacts of the attack. Even though Anna and Miroslav did not experience another attack after taking out the insurance, knowing that they have financial protection provides them with reassurance. Hypothesis H1 is therefore confirmed, with insurance contributing to the reduction of financial losses after an incident.

Hypothesis H2: Local governments with a higher level of security measures implementation achieve better cyber insurance terms.

All three mayors who implemented advanced security measures stated that this led to more favorable insurance terms. Insurance companies appreciated their proactive approach and offered lower insurance rates and a wider range of coverage. Hypothesis H2 is therefore confirmed, as the level of security measures positively affects insurance terms.

Hypothesis H3: Training employees to recognize cyber threats reduces the frequency of successful cyber attacks on local governments.

Anna and Miroslav stated that regular employee training significantly increased awareness of cyber threats and reduced the risk of successful attacks. This training helped employees recognize phishing emails and other suspicious activities, which contributed to the overall security of the municipality. Hypothesis H3 is therefore supported, with training being an effective tool to reduce the risk of attacks.

Hypothesis H4: Cyber insurance supports faster recovery and restoration of local governments' operations after an incident.

Jana confirmed that the insurance allowed them to restore their systems faster and provided expert support in crisis management. This minimized the impact on service provision to citizens and helped to quickly restore public trust. Hypothesis H4 is therefore confirmed, as insurance contributes to more effective management of the consequences of attacks.

Hypothesis H5: Municipalities and districts that have comprehensive security policies and procedures in place report lower overall costs of cyber incidents in the long term.

Although Jana suffered high financial losses despite the measures in place, it is important to note that these measures were implemented after the attack. Anna did not experience further attacks after the implementation of comprehensive measures, indicating potentially lower costs in the long term. Hypothesis H5 is therefore partially supported, with timely implementation of comprehensive security measures potentially contributing to reducing the costs associated with cyber incidents.

3.1 Interpretation of the results

Cyber insurance is still an unknown or inaccessible tool for many Slovak municipalities. The research results show that the greatest need for protection is in smaller municipalities, which face a lack of resources to implement comprehensive security measures. These municipalities are also the most vulnerable to cyber threats, such as phishing or ransomware attacks, because they lack sufficiently trained personnel and technical support.

One of the solutions we propose based on the findings from the interviews and research is the creation of simple "starter packages" of cyber insurance, which would be tailored to smaller municipalities. Such packages could include:

Basic coverage for the most common threats, such as phishing attacks or malware. The insurance could cover the costs of restoring systems, removing malware and restoring basic services.

– **Legal assistance and advice in the event of a leak** of sensitive data or if the municipality faces legal claims from citizens.

– Data backup support to ensure that critical data can be quickly restored even in the event of a successful attack.

These packages should be affordable, with premiums tiered according to the size of the municipality, its budget and risk profile. Insurance companies could also offer more favorable terms to municipalities that have implemented at least minimal security measures, such as regular data backups or the use of anti-virus software.

Insurance financing options

The interviews revealed that one of the main obstacles to taking out cyber insurance is the limited budget of municipalities. If the insurance were available at a "reasonable price", or if the state or the European Union provided them with financial support. This proposal is also supported by the recommendations of the European Commission (2023), which propose the introduction of grant programs to support cybersecurity. One option to reduce the financial burden on municipalities could be:

• State subsidies for insurance, which would cover part of the cost of insurance premiums, especially for smaller and financially weaker municipalities.

• **European grants aimed** at increasing cyber resilience, which could also include support for taking out insurance.

• **Collective insurance funds** that would allow several municipalities to pool their resources to finance insurance.

These measures could be implemented as part of a broader strategy to increase cybersecurity at regional and national levels.

Insurance with an emphasis on prevention and education

Cyber insurance that would include preventive measures could play a key role not only in covering the costs associated with incidents, but also in reducing the likelihood of them occurring in the first place.

Regional collective insurance

Collective insurance could be based on the cooperation of several municipalities within a region. This model would include:

Common insurance fund

Shared resources

Crisis coordination

3.2 Simpler processes and more transparent insurance products

One of the biggest obstacles we identified in the survey is the financial unavailability of cyber insurance for smaller municipalities. Despite the fact that these municipalities are among the most vulnerable to cyber attacks, their budgets are often strained by priority investments in infrastructure or social services.

The state and the European Union have already proven in the past that they are able to support security initiatives in areas such as the protection of critical infrastructure or digital inclusive solutions.

One of the main problems we identified in the survey and during interviews with mayors is the complexity of insurance processes and the lack of transparency of insurance products. **Many municipalities, especially smaller ones,** feel discouraged by complicated contract terms and conditions and the complex process of concluding insurance contracts.

Conclusion

Cybersecurity of Slovak municipalities is becoming an increasingly urgent topic that cannot be ignored. The aim of this survey was to examine the state of cybersecurity of municipalities, identify their most common problems, verify hypotheses regarding the types of cyber attacks and impacts, and at the same time propose solutions in the form of preventive measures and effective use of cyber insurance.

The survey showed that Slovak municipalities face significant cyber threats, the most common of which are phishing attacks, which accounted for up to 66.67% of all reported incidents. This statistic clearly confirms the assumption that phishing is the dominant type of attack, which is in line with the theory of Jakobbson and Myers (2006), who point out its simplicity and effectiveness.

To a lesser extent, municipalities also encounter ransomware and malware attacks, which, however, have a significantly greater impact on their

functioning. Interviews with mayors revealed that these attacks not only crippled the provision of public services, but often also reduced citizens' trust in the municipality's ability to protect their data. We thus confirmed the hypothesis that cyber attacks have not only technical, but also social and economic consequences that significantly affect the functioning of municipalities.

The economic impact of the attacks turned out to be significant, with municipalities reporting direct financial losses ranging from a few thousand euros to tens of thousands of euros. These losses included the costs of system restoration, legal services and compensation for service interruption. The hypothesis that cyber attacks have significant financial consequences was clearly confirmed.

Cyber insurance has proven to be an important tool for managing cyber risks, but research has also identified its weaknesses. Many municipalities, especially smaller ones, reported that insurance was financially unaffordable or administratively complex for them.

References:

1. HARLEY, D. 2007. The AVIEN Malware Defense Guide for the Enterprise. pp. 45-60.

2. SINGER, P. W., FRIEDMAN, A., 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know.

3. RADU, R. 2020 Understanding cyberattacks: Origins, Evolution and Implications. with 3-5..

4. KHAN, M., B., SHARIF M. 2019. A Study of Malware and its Detection Techniques.. 2019. p. 145-158.

5. HAWKINS, K., W., PRICE H., WILLIAMS. B., M. 2022. A Comprehensive Overview of Cybersecurity Threats and Defense Strategies. with 93-105.

6. PAGLIERY, J. 2017. Ransomware: Unlocking the Virus that Hijacks your Files.

7. KRUSE, C., et al. 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends.. p. 17-20.

8. MAO, Z., SCHMIDT A.M.. 2021. DDoS Attacks: Classification and Countermeasures

9. HARLEY, D. 2007. The AVIEN Malware Defense Guide for the Enterprise,. with 22-75.

10. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA). 2023. Ransomware Guide.

11. VINAYAKUMAR, R., et al. 2019. Deep learning for intelligent intrusion detection systems: A review. IEEE Access. with 23-24.

12. EUROPEAN COMMISSION. 2023 Cybersecurity in the EU.

13. IBM. 2023. Cost of a Data Breach Report 2023.