LEX LOCALIS - JOURNAL OF LOCAL SELF-GOVERNMENT
Vol. 20, No. 1, pp. 161 – 192, January 2022

Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done

ANETA CHODAKOWSKA, SŁAWOMIRA KAŃDUŁA, & JOANNA PRZYBYLSKA

Abstract Although cybersecurity is an important and complex issue that should be addressed by all government levels, so far little research has been devoted to cybersecurity at the local level. Existing literature lacks information on whether municipalities have implemented cybersecurity policies, if such policies are applied in practice and what they encompass. A CAWI method was used to collect the required data. The results indicate that while most municipalities have a document defining their security policy, they do not always apply it in practice. There is still little awareness regarding countering cyber-attacks. Therefore, more emphasis should be placed on such issues as: integrating cybersecurity policies into local government management, the rising threat of cyber-attacks, consultations with security auditors, and cybersecurity management training. Based on all Polish municipalities, the research described in this paper partly fills the identified gap.

Keywords: • cybersecurity • local government • public sector • information security • Poland

CORRESPONDENCE ADDRESS: Aneta Chodakowska, Ph.D., Assistant, Poznań University of Economics and Business, Department of Public Finance, 61-875 Poznań, al. Niepodległosci 10, Poland, email: aneta.chodakowska@ue.poznan.pl. Sławomira Kańduła, dr hab., Associate Professor, Poznań University of Economics and Business, Department of Public Finance, 61-875 Poznań, al. Niepodległosci 10, Poland, email: slawomira.kandula@ue.poznan.pl. Joanna Przybylska, Ph.D., Assistant, Poznań University of Economics and Business, Department of Public Finance, 61-875 Poznań, al. Niepodległosci 10, Poland, email: joanna.przybylska@ue.poznan.pl.

https://doi.org/10.4335/20.1.161-192(2022)
ISSN 1581-5374 Print/1855-363X Online © 2021 Lex localis
Available online at http://journal.lex-localis.press.

1 Introduction

In recent years information and communication technologies (ICT) have become widespread and integral in the function of local governments, due to the shift of public entities to the standards of economy 4.0. The reasons for the need to implement digital technologies by public entities can be found in two dominant theories – technology push and demand-pull, which were coined as early as the 1950s and 1960s to explain technological changes taking place in world economies (Peters et al., 2012). According to the first theory, public authorities can initiate changes through policies that trigger innovativeness among business entities. In turn, the concept of demand-pull explains that public authorities, including local governments, may respond to digital innovation requirements reported both by enterprises and individuals (Nemet, 2009).

In order to adapt to the emerging digital economies, local governments are themselves undergoing similar transformations in terms of their services, processes, resources, organisational culture, and competencies in order to (Polityka Cyfrowa Miasta Stołecznego Warszawy, 2020): (1) improve accessibility and quality of public services, (2) streamline the function of local government, (3) support the processes of strategic and operational decision-making, (4) increase the transparency of local government operations, (5) and engage residents in the life of the local government community through ICT technologies. Such transformations are aimed to achieve sustainable development goals.

Both the creation of telecommunication infrastructure and networks, as well as ensuring their security for all users, requires considerable financial expenditure. This creates a problem, as – on the one hand – private entrepreneurs are not always interested in incurring such costs, and – on the other – providing these goods and services on market terms would limit access to them for part of society. Therefore, these tasks must be taken over by public administration bodies acting in the public interest (Grossmann et al., 2013), and their aim should be to counteract the so-called digital exclusion. However, the increasingly widespread use of ICT technologies creates an additional problem related to ensuring ICT or cybersecurity in the economy, including local government units. The number of reported cybersecurity incidents and cyber-attacks on public administration offices is growing each year. These entities are therefore obliged to ensure the security of ICT networks and systems (Chałubińska-Jentkiewicz, 2021c). It is necessary to develop security software protecting against cyber-attacks, and to appoint persons responsible for monitoring compliance with cybersecurity policies (Chatfield & Reddick, 2019). Security and cybersecurity become key issues during emergencies, such as the recent COVID-19 pandemic. For this reason, the subject matter of the article should be considered as particularly important and topical.

In addition, despite the recognised need to implement cybersecurity strategies and legal norms, so far there has been little research verifying the adopted solutions in practice or analysing actual examples of cybercrime in public entities, especially at the local government level. The existence of this research gap has prompted the authors to formulate the research objective presented in this paper, consisting in diagnosing the state of cybersecurity in local government units of Polish municipalities, as well as the awareness of local authorities regarding cyber-attacks and the need to ensure cybersecurity at the municipal level. The use of Polish municipalities, as a case study, was dictated by several factors. First of all, the issue of cybersecurity at the local government level in Poland has not been sufficiently investigated so far. The existing literature on the subject lacks information on whether Polish municipalities have implemented a cybersecurity policy, whether such a policy is applied in practice and what it consists of. Secondly, there is also no data on the obstacles during the processes of creating and implementing cybersecurity policies in terms of the financial, organisational, and human resources aspects. Finally, so far it has not been verified whether the legal solutions adopted in recent years at the central level in order to reduce the risk of cyber-attacks at the local level are effective. Therefore, the research presented in this paper adopted three research hypotheses. The first one (H1) concerns the awareness of local government employees of the risks of cybercrime and whether the level of such awareness is related to the number of actions taken to prevent it. The second hypothesis (H2) verifies whether the legal requirement to implement an information security management system has had an impact on the reduction of security breaches. Finally, the third hypothesis (H3), is detailed analyses on the current legal solutions and the effects of periodic risk analysis on the loss of integrity, confidentiality, and availability of information.

The objective of the article was achieved through literature research and analysis of legal acts and guidelines on cybersecurity in local government units that came into force as of 1 May 2021. The research hypotheses were verified on the basis of a questionnaire conducted among local government units in Poland in 2020. The questionnaire provided information about the level of awareness of local government employees regarding existing threats to security, implemented information security management policies, information security incidents, and cybersecurity management in municipalities in Poland.

The article is divided into four sections. The first section focuses on the literature review on cybersecurity and cybercrime, as well as the responsibilities of local governments in this regard. The second one describes the research method and data sources. The third section of the article presents the results of the survey on the state of cybersecurity at the municipal level in Poland. Finally, conclusions from the conducted research, as well as recommendations and directions for further research are presented in section four.

2 Literature overview

2.1 Cybersecurity in local governments

In the narrow sense cybersecurity is the practise of protecting data and information (resources). Broadly speaking, it is about protecting: digital content, ICT networks, business devices and transmission of content via the Internet. It is also important to protect clients and their computers (Chałubińska-Jentkiewicz, 2019). Cybersecurity is currently regarded as one of the greatest socio-technological challenges that public institutions are currently facing (de Bruijn & Janssen, 2017). It has strategic importance not only for the proper functioning of the state and local government, but also for the private companies and residents using e-administration services (Karpiuk, 2021a). The need to ensure cybersecurity in public administration functions, including local government units, is increasingly emphasised in the literature (Chałubińska-Jentkiewicz, 2021b), government documents, and reports prepared by independent institutions (Ruohonen, 2020; Salminen & Hossain, 2018). In spite of this, the actual awareness of the threats both among public authorities and the public is limited (de Bruijn & Janssen, 2017). This also seems to be confirmed by the fact that there is still relatively little research on cybercrime and cybersecurity, especially at the level of local governments (Kańduła & Przybylska, 2020; KnowBe4, 2020; Schallbruch & Skierka, 2018). A major challenge for researchers is the lack of official statistics on the number and types of cyber-attacks carried out in local government units and the capability of central and local authorities to counter such attacks. Some of this information is confidential.

The advancement of local governments in terms of digital transformation, i.e. the level of use of ICT technologies in their activities, is gradual (Janowski, 2015; Reddick, 2004) and the transition to the subsequent, more advanced stages is accompanied by increased concerns about the ability to ensure the confidentiality of the processed data (D'Agostino et al., 2011). Ensuring the security of municipal IT systems is a complex problem, which is critical both from the point of view of municipal authorities and officials, as well as the residents themselves. Local government units are, on the one hand, expected to ensure the transparency of their operations and on the other, the confidentiality of the data of local residents and businesses. The results of a survey conducted among county officials in Florida, USA, indicate that achieving both objectives requires more financial resources, better-prepared staff, as well as more advanced equipment and software. What is also necessary is to spread awareness of potential risks among officials, develop clear cybersecurity policy standards and procedures, and ensure strict law enforcement (Macmanus et al., 2013).

Local government units are considered to be legal entities and are legally guaranteed independence of action. However, in terms of cybersecurity, they should cooperate not only with one another, but also with representatives of state administration and government agencies. (Hatcher et al., 2020; Wolff & Lehr, 2018). The exchange of experience, joint development of systems, as well as the use of economies of scale are the most important aspects local governments should pay particular attention to when considering cooperation. This is emphasised by (Kesan & Zhang, 2019). The authors observe that in recent years small local government units have increasingly come under cyber-attack, and should, therefore, devote more resources and invest in technologies protecting against this kind of threat. At the same time, the authors acknowledge that these entities are frequently dealing with the problem of insufficient financial resources to build an adequate security system on their own. In addition, (Finster & Baumgart, 2015) point out that the greatest threat affect those communities that define themselves as "smart". Smart villages and smart towns rely, to a great extent, on the use of various applications, which – in case of security gaps – can result in leakage of sensitive information about the residents. Similar conclusions are presented by (Szabó, 2019).

Among the few authors who deal with the state of local government cybersecurity are (Ibrahim et al., 2018), who presented a case study of Western Australia. The conclusions of their research are quite optimistic – Australian municipalities are relatively well prepared to prevent cybercrime and local government employees are appropriately trained and informed about their responsibilities with regard to information security. What is lacking, however, are appropriate policies, procedures, and technologies to help protect information systems.

A survey conducted by Hatcher et al. (2020) on a group of 168 civil servants working in different cities in the US found that most cities have prepared a document that outlines security policies, but do not keep records of cyber-attacks. The level of cooperation between cities, external auditors, and IT security policy specialists is far from satisfactory, too. One possible reason is insufficient funding, even in a city as large as Atlanta. Financial obstacles also prevent conducting adequate cybersecurity training. The findings and recommendations of the above-mentioned researchers (to which we refer in the discussion) confirm the observations made by (Norris et al., 2019), although it seems that the overall assessment of the readiness of US municipalities to counter cyber-attacks that emerge from the first nationwide survey of the state of cybersecurity in US municipalities (Norris et al., 2020) is less optimistic.

Some authors choose to focus on the state of security of selected spheres of local government activity. For example, (Zhao & Zhao, 2010) examine the security of local government websites. In turn, (Fusi & Feeney, 2018) focus on electronic monitoring of employees. The authors emphasise that the monitoring of online activities of local government employees is introduced to prevent the employees from unintentionally violating the security of the local government unit.

In 2015, a survey was conducted among 200 officials responsible for ICT in local governments in Poland (*Jak to Jest z Cyberbezpieczeństwem w Samorządach?*, 2015). The respondents assured that the offices supervised by them are well prepared to counter cyber-attacks, although the primary defence tool used was anti-spam software. According to 62% of the respondents, the greatest obstacle to improving cybersecurity was the lack of sufficient funding. Seventeen percent indicated little awareness of the problem at higher administrative levels, while only 13% blamed the problem on the lack of central IT security strategy and standards. A year later, a survey on the state of cybersecurity was conducted in municipalities of the Łódzkie Province. Information was collected on the implemented information security management systems, information security incidents, and methods of cybersecurity management in the offices (Lisiak-Felicka & Pytko, 2017). The authors stress that there was little interest from municipalities in sharing their experiences in this area.

The identified research gap reflected in a shortage of empirical analyses based on the actual state of cybersecurity in local governments, rather than solely on existing documents or implemented strategies, prompted the authors to undertake research in this area. This paper focuses on Polish local government units, but given the current deepening globalisation and blurring of borders in the online world, it can be assumed that local governments of other European countries are facing similar challenges.

2.2 Institutional background – public tasks of Polish local government units in the field of cybersecurity

The development of ICT technologies has made public administration responsible not only for the quality and maintenance of technical infrastructure in a conventional sense but also for ICT networks (Chałubińska-Jentkiewicz, 2021a) which entails new threats. Thus, ensuring the security of IT systems used by local government units (LGUs) to perform public tasks has recently become one of the most important challenges faced by these entities.

Pursuant to Polish law, in order to satisfy the collective needs of the local community a LGU may (Act of 7 May 2010):

1. build or operate (public) telecommunication infrastructure and networks and acquire rights thereto;
2. provide access to telecommunication networks or infrastructure;
3. use own telecommunication infrastructure and networks in order to provide services to: a) telecommunication entrepreneurs, b) selected state organisational units and certain state legal persons, and c) end-users (entities using publicly available telecommunication services or requesting the provision of such services to satisfy their own needs).

In Polish law, cybersecurity is defined as the resistance of IT systems to any actions that violate confidentiality, integrity, availability, and authenticity of processed data or related services offered by these systems (Act of 5 July 2018). In order to provide services via the Internet, LGUs need to ensure the security of such data in IT systems. What is particularly important in this context are cybersecurity programmes and policies, the development of which is one of the tasks of municipalities in Poland.

Municipalities have the most extensive knowledge on the matters concerning a local community, but the legislator has not awarded them with any special status (Karpiuk, 2021b). They are among the public entities which have been imposed with certain obligations due to their role in the National Cybersecurity System (NCS), which is an element of crisis management referred to by Kostrubiec (2021b) and Karpiuk (2021c). One of the tasks of LGUs is the appointment of a person responsible for maintaining contact with the entities of the NCS (Kostrubiec, 2021a). This should be a person responsible for ICT systems and information security in the office. When it comes to small LGUs, due to the limited number of duties, it may be the same person who performs the function of a personal data protection inspector. Such a person may only maintain contact with other entities of the NCS through information systems that are used by these entities to perform public tasks (Act of 5 July 2018).

It is also necessary to prepare structures and procedures that will enable an appropriate response to various incidents, i.e. events that have or may have a negative impact on cybersecurity. As part of the adopted solutions, it is essential to (1) ensure incident management (handling of incidents, searching for connections between incidents, removing reasons for their occurrence, and developing conclusions from incident handling), (2) report incidents to the relevant entity within 24 hours of their detection, and (3) ensure incident and critical incident handling in cooperation with the relevant entity by providing necessary data, including personal data (Act of 5 July 2018; Świtała, 2019).

LGUs are also required to ensure that the entities, for which they carry out public tasks, have access to information to make them aware of possible cybersecurity threats and apply effective ways to protect themselves against these threats. LGUs must additionally bear in mind that the National Cybersecurity System Act also covers entities supervised by them or in which they have shares. This applies in particular to entrepreneurs who can be defined as key service operators in such sectors as: energy, transport, banking and financial markets infrastructure, health care, drinking water supply, and digital infrastructure. In LGUs, these may include hospitals, water supply and sewage companies, airport operators, etc. These entities have the greatest responsibilities in terms of building cybersecurity (Act of 5 July 2018).

LGUs are also obliged to develop, establish, and subsequently implement, operate, and monitor an information security management system to ensure confidentiality, availability, and integrity of information, taking into account such required characteristics as authenticity, accountability, indisputability, and reliability. The legislation details actions that must be taken in order to ensure the security of information systems. One of the key requirements, which is at the core of a well-functioning information security management system, is to conduct periodic risk analyses in terms of the loss of information integrity, availability, or confidentiality and to take actions to minimise this risk, according to the results of the analysis (Regulation of April 12 2012). As a preventive measure, LGUs are, therefore, obliged to regularly carry out risk analyses concerning the state of cybersecurity, in order to reduce the likelihood of cyber threats.

LGUs also have to face the challenge of coordinating obligations imposed on them under the Cyber Security Act with those resulting from other regulations, in particular from GDPR, the Act on the Computerisation of the Operations of the Entities Performing Public Tasks (including its implementing act – the National Interoperability Framework) or the Act on the protection of classified information (Act of 17 February 2005; Regulation of 12 April 2012; Regulation of 27 April 2016). All these law acts are interconnected and it is important not to interpret them separately. ICT system security, information management and protection, and personal data protection must form a coherent system.

The greatest risk for cybersecurity is currently posed by malware, hacking, unauthorised access, or collection of information (Wojciechowska-Filipek & Ciekanowski, 2019). The solutions implemented to minimise these threats have certain limitations. The most frequently mentioned problems are financial limitations, which are particularly acute in the case of small LGUs. Difficulties in obtaining financing prevent these LGUs from implementing basic technical security measures, but also prevent the recruitment of experts in the field of information security (Eisenstein, 2019).

In the common understanding, cyber threats are usually equated with hacker attacks. Meanwhile, it turns out that mere human carelessness, often resulting from a lack of awareness and proper education may pose an even greater threat (Brumfield, 2019). According to a report by the Supreme Chamber of Control issued in May 2019 concerning cybersecurity in local governments, more than 80 percent of the audited offices' irregularities were found in the management of user rights in IT systems. Experts agree that carelessness and a certain degree of credulity, on the part of officials, are not only reflected in the casual sharing of passwords, but also in the opening attachments of suspicious emails or the use of flash drives of unknown origin on official computers. In all these cases, the consequences of such careless actions can be very serious (NIK, 2019).

3 Research

3.1 Hypotheses and methodology

Based on the analysis of the literature on the subject and the legal solutions implemented in Poland aimed at reducing the risk of cyber-attacks, three research hypotheses have been formulated:

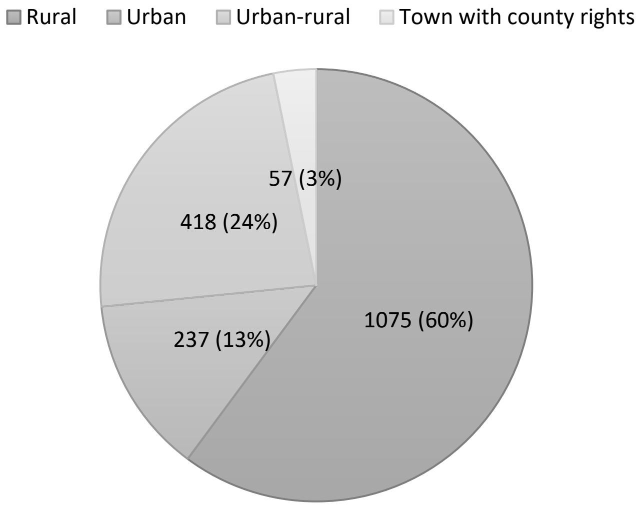
- H1: Municipalities that perceive cybercrime as little or no threat are less likely to take measures in order to reduce the risk of cyber-attacks.
- H2: Municipalities with an implemented information security management system are less likely to fall victim to a security violation.
- H3: Municipalities which carry out periodic analysis of the risk of loss of information integrity, confidentiality, and availability are less likely to fall victim to a security violation.

The survey was conducted in the period from 16 March to 15 April 2020 with the use of the CAWI method (Computer Assisted Web Interview). A request was sent to complete an electronic questionnaire to the offices of all municipalities in Poland.

The survey covered a total of 2477 municipalities – 1532 rural, 643 urban-rural, and 302 urban ones, including 66 municipalities being towns with county rights (Fig. 1). Responses were obtained from 1787 municipalities (response rate of 72.1%), which can be considered a representative sample of the entities in question.

60.0% of the responses obtained were from rural municipalities, followed by urban-rural (24.0%), urban ones (13.0%), and cities with county rights (3.0%). The largest number of municipalities were from the Mazowieckie (13.5%), Małopolskie (9.0%), Lubuskie (8.5%), and Śląskie Provinces (8.4%). With regards to the number of residents, the majority of the respondents were municipalities with up to 10 000 residents (64.4%). The second largest group were municipalities with 10 000-20 000 residents (20.9%). The research group consisted mainly of municipalities with average income below 3000 PLN per person (36.5%), followed by municipalities with revenue per person between 4000-4500 PLN (18.1%) (Table 1).

Figure 1: Types of municipalities.



Source: Own elaboration based on research.

In order to verify the research hypotheses presented in the article, the obtained responses were tested using Pearson's Chi-squared Test. This test is commonly used for categorical data to test the hypothesis that the frequency distribution of particular events observed in the analysed data is consistent with a particular theoretical distribution. Therefore, it tests whether the observed differences occurred by chance (Heeringa et al., 2017).

3.2 Questionnaire results and their analysis

This part of the paper firstly presents the results of the questionnaire, which served as the basis for verifying the formulated hypotheses.

Among the examined municipalities, only 3.6% were recognised as key service operators. Persons appointed to maintain contact with the national security system entities in the municipality were mainly either IT staff (40.6%) or mayors (40.6%). The information security management system was implemented in 76.9% of the municipalities surveyed, while 82.2% of the systems were accredited for compliance with the PN-ISO/IEC 27001:2017-06 standard. The reason for the lack of such a system in the remaining municipalities was mainly lack of sufficient financial resources (37.5%) and lack of systems for electronic document circulation (24.9%). The municipalities declared that they would be persuaded to implement an information security management system if they were granted additional funds for this purpose by the government administration (52.3%) or if an electronic document circulation system was introduced (19.6%) (Table 2).

According to the majority of the respondents, cybercrime poses a medium (34.9%) or high (31.4%) threat to the office. Only 3.5% of the respondents held the view that it poses no such threat. Most (78.5%) municipal offices declared that they regularly conduct an analysis of the risk of loss of integrity, confidentiality and availability of information. The remaining municipalities did not conduct it due to the lack of financial resources (35.6%) or the lack of a need for such an analysis (24.7%). An up-to-date and comprehensive electronic inventory of IT equipment was carried out in 81.0% of the examined municipalities. An annual internal audit of information security was carried out in municipalities by an external service provider (44.9%) or by an internal auditor (30.1%). A quarter (25.0%) of the municipalities did not undertake such an audit at all, the reason – in most cases – being the lack of sufficient financial resources (59.3%). A majority (86.7%) of the municipal offices did not suffer any information security incidents in 2017-2019, while in 10.6% of the municipalities up to 5 such incidents occurred. However, as many as 44.4% of those offices did not report that fact (Table 3).

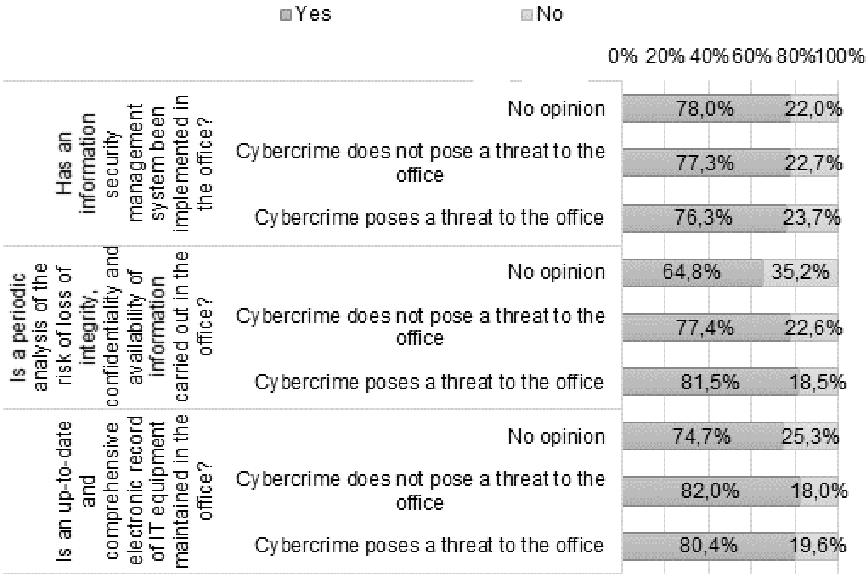
The most frequently mentioned areas that the respondents felt were most susceptible to cybercrime were personal data (54.1%), employees (57.5%), and employee equipment (44%), while cloud infrastructure (8.1%) was regarded as the least vulnerable. The most frequent cases of cybercrime in the examined group involved spam (79.1%), phishing (26.5%), and malware (26.5%). Undertaken measures against cybercrime were mainly antivirus software (96.3%), firewall (89.0%), spam blockers, and filters (69.2%). Only a small number of municipalities used SIEM (2.7%), VOIP encryption (5.4%), and early warning systems (7.8%) (Table 4).

In most cases, the offices had an internal cybersecurity management system implemented (88.4%). In the period from 2017 to 2019, cybersecurity training was organised for all employees in 50.5% of the examined municipalities, while in 9% of them, it was conducted only for management staff. No such training was conducted in 40.6% of the municipalities, partly due to the lack of funding (54.3%) or no need to do so (38.2%). Only 11.4% of the municipalities in question were insured against the risk of cyber-attack, while 53.5% of them planned to purchase insurance in this regard (Table 5).

The results of the questionnaires allow for a diagnosis of the state of cybersecurity in the analysed municipalities, as well as verification of the adopted research hypotheses. According to the first one (H1), municipalities that perceive cybercrime as little or no threat are less likely to take measures in order to reduce the risk of cyber-attacks. The results of the analyses indicated that the assessment of the risk posed by cybercrime depended on whether a periodic analysis of the risk of loss of integrity, confidentiality, and availability of information was carried out ($p < .01$)

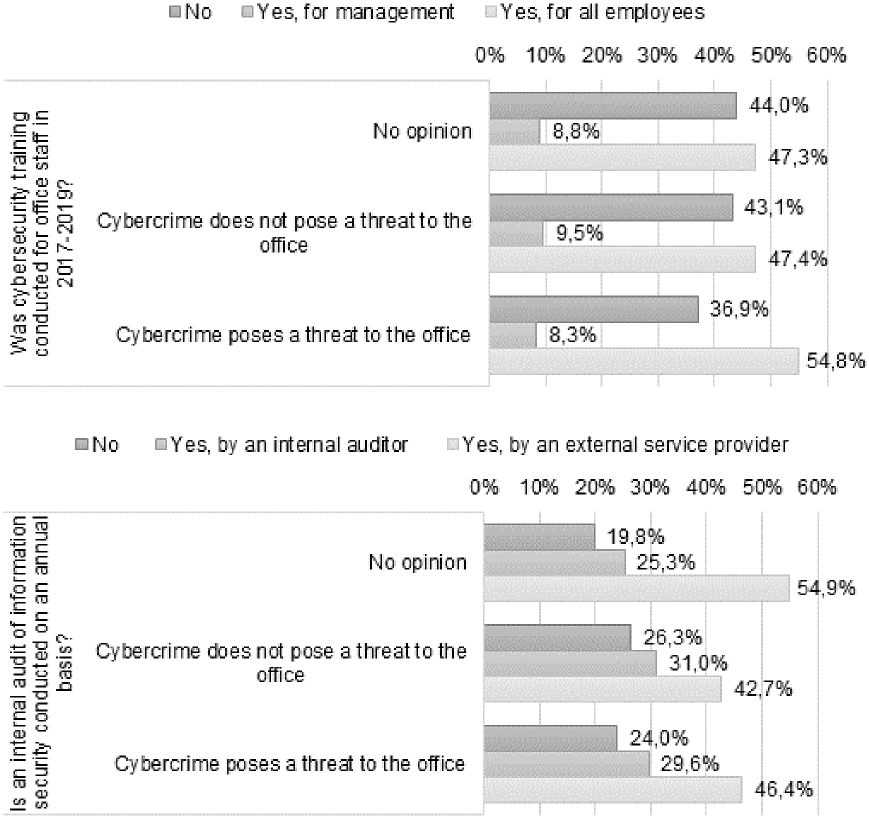
and whether cybersecurity training was organised for the employees of municipal offices (p < .05). The perception of the threat of cybercrime as low was positively correlated with less frequent periodic analysis of the risk of loss of integrity, confidentiality and availability of information as well as less frequent cybersecurity training for office staff. No correlation was observed between the assessment of the threat posed by cybercrime and the implementation of an information security management system, the maintenance of complete and up-to-date electronic records of IT equipment, and the performance of an annual internal information security audit (Table 6, Figures 2-4).

Figure 2: Correlation between the perception of cybersecurity as a threat, implementation of information security management systems, conducting periodic risk analyses and maintaining up-to-date and comprehensive electronic records of IT equipment.



Source: Own elaboration based on research.

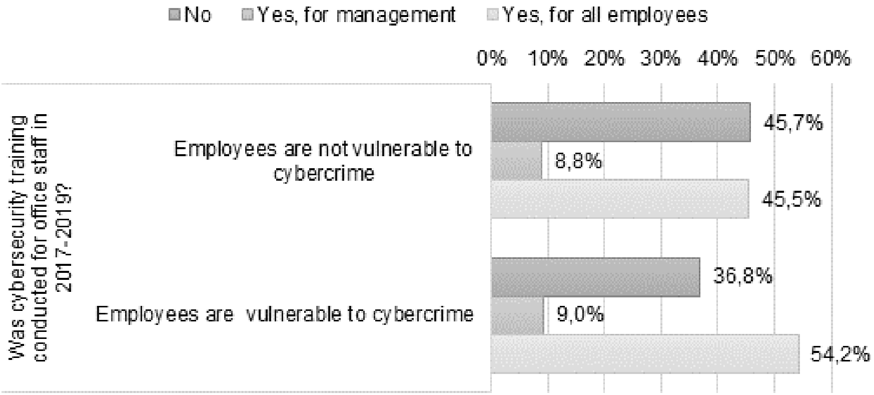
Figure 3: Correlation between the perception of cybersecurity as a threat, conducting internal audits, and organising training for employees of municipal offices.



Source: Own elaboration based on research.

Using Pearson's χ2 test analysis, a correlation was also found between the opinion that employees pose a threat to cybersecurity and the frequency of organised staff training $\chi^2(2) = 15.23$; $p < .001$; $V = .09$. Municipalities that expressed the opinion that their own employees may pose a threat to the cybersecurity of the office tended to implement cybersecurity training for the staff more often (Fig. 8).

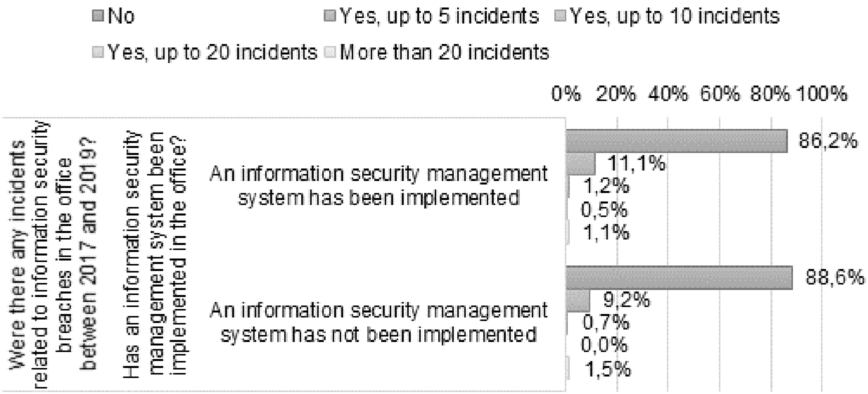
Figure 4: Correlation between the perception of employees as vulnerable to cybercrime and the implementation of cybersecurity training for the staff.



Source: Own elaboration based on research.

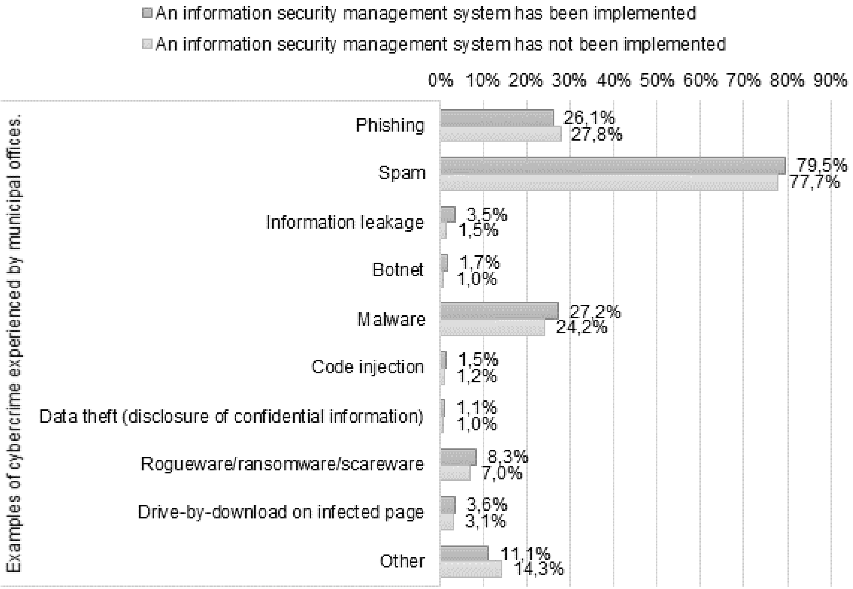
Pearson's χ^2 test analysis was also used to examine whether municipalities with an implemented information security management system are less likely to fall victim to security violation (H2). The conducted analysis did not confirm any correlation between the implementation of an information security management system and the frequency of security breaches in the office between 2017 and 2019 ($p > .05$). It was only shown that offices where an information security management system was implemented were more likely to experience information leaks ($p < .05$). No more other statistically significant correlations were found between the implementation of an information security management system and the occurrence of cybercriminal activity (Table 7, Figure 5-6).

Figure 5. Correlation between the implementation of an information security management system and the occurrence of security breaches.



Source: Own elaboration based on research.

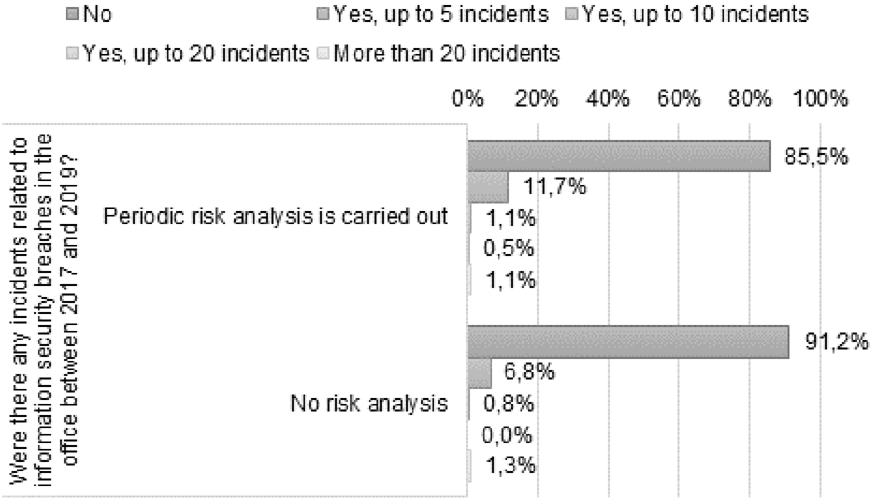
Figure 6: Correlation between the implementation of an information security management system and the occurrence of security breaches.



Source: Own elaboration based on research.

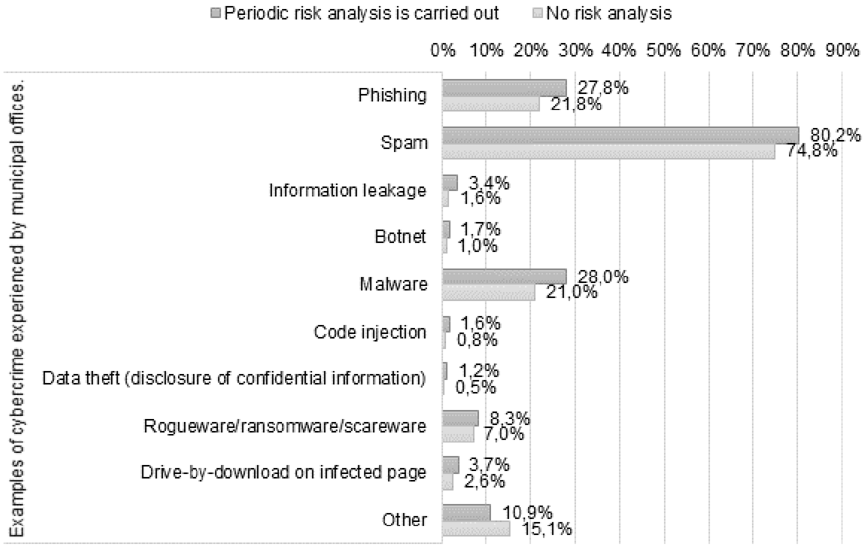
The purpose of the last, most detailed hypothesis based on the centrally implemented legal solutions, was to verify whether municipalities which carry out periodic analysis of the risk of loss of information integrity, confidentiality, and availability are less likely to fall victim to a security violation, or – in other words – to verify whether the centrally adopted law, which LGUs are obliged to comply with, meets its objectives (H3). The results are presented in Figure 7 and Table 8. The research showed that conducting a periodic analysis of the risk of loss of integrity, confidentiality, and availability of information in municipal offices was correlated with the occurrence of incidents related to information security breaches (p < .05). Offices that conducted such analyses were more likely to report information security incidents, but the differences were not significant. It was also found that conducting the mentioned analyses was statistically significantly correlated with the occurrence of instances of phishing p < .05, spam p < .05, malware p < .01, and other cybercriminal activities p < .05 in offices. In the case of municipalities that conducted a periodic analysis of the risk of loss of integrity, confidentiality, and availability of information, spam, phishing, and malware were more frequent, while other types of cybercrime less common than those mentioned in the list.

Figure 7: Correlation between conducting periodic analyses of the risk of loss of information integrity, confidentiality and availability and the occurrence of security breaches



Source: Own elaboration based on research.

Figure 8: Correlation between conducting periodic analyses of the risk of loss of information integrity, confidentiality and availability and the occurrence of security breaches.



Source: Own elaboration based on research.

4 Discussion

Municipalities are fundamental pillars of public administration. Their residents often, and increasingly, make use of electronic means to deal with their day-to-day affairs. Awareness and adequate competencies in the field of cybersecurity of local administration employees are crucial for the proper implementation of public services.

The majority of municipalities in Poland have an adequate information security organisation, and an information security system has been developed and implemented in most offices. Having a formally approved security policy in place is crucial, as stressed by (Hatcher et al., 2020). In addition, most municipalities carry out an internal information security audit every year. Nevertheless, some of the municipalities included in the survey have not taken sufficient measures to prevent information security incidents and have not carried out mandatory information security audits. Failure to meet the above-mentioned obligations indicate not only a lack of awareness of threats related to cybercrime, but also a lack of knowledge regarding legislation in this regard.

The objective of the first research hypothesis (H1) was to verify whether municipalities that perceive cybercrime as little or no threat are less likely to take measures in order to reduce the risk of cyber-attacks. The research found that the perception of the threat of cybercrime as low was positively correlated with less frequent periodic analysis of the risk of loss of integrity, confidentiality, and availability of information as well as less frequent cybersecurity training for office staff. No correlation was observed between the assessment of the threat posed by cybercrime and the implementation of an information security management system, the maintenance of up-to-date and complete electronic records of IT equipment, and the performance of an annual internal information security audit. Unfortunately, the results of the survey are not optimistic in this respect and demonstrate the need to take appropriate measures to spread awareness among managers and employees of municipal offices of cybersecurity, which is also pointed out by (DiNapoli, 2016; Eisenstein, 2019; García Zaballos & González Herranz, 2013).

The conducted research did not show a correlation between the implementation of an information security management system and the assessment of the occurrence of security breaches in offices between 2017 and 2019 (H2). It was only shown that offices where an information security management system was implemented were more likely to experience information leaks. In-depth research would have to be carried out in order to determine its causes. No other correlations were identified between the implementation of an information security management system and the occurrence of cybercriminal activity.

The third, most detailed hypothesis (H3), according to which municipalities which carry out periodic analysis of the risk of loss of information integrity, confidentiality, and availability are less likely to fall victim to a security violation, was not confirmed. The research showed that conducting a periodic analysis of the risk of loss of integrity, confidentiality, and availability of information in municipal offices was not correlated with the occurrence of incidents related to information security breaches. On the contrary, in municipalities where such analysis was carried out, incidents such as spam, phishing, and malware were more frequent, although the differences were not large. There are two possible reasons to explain that. On the one hand, the more frequent detection of cybersecurity breaches may be due to the fact that they were detected thanks to existing solutions. Municipalities that do not perform threat analysis may not be aware of their occurrence, as they are unable to identify them. The observed correlation may also be the result of taking action aimed to increase cybersecurity only after cybersecurity incidents have occurred; the greater number of incidents the more frequent verification of the integrity, confidentiality, and availability of information to ensure that it is adequately protected. In such cases, the actions undertaken by municipalities are not preventive, but corrective in nature. In order to unambiguously determine the cause-effect relationship between the indicated phenomena, analyses of causal inference would have to be carried out.

The research presented in this paper has allowed us to identify the following gaps in the cybersecurity of municipalities that should be addressed: lack of a security policy, lack of a habit of reporting security-related incidents, lack of security audits, lack of insurance against the risk of cyber-attacks, and lack of appropriate staff training.

Attacks and incidents in cyberspace on various scales and with various consequences, have become a new reality and pose a genuine threat not only to individual citizens and companies, but also to LGUs and the state. Many of the surveyed municipalities are – at least partially – prepared for these attacks, but there is still a great number of municipalities that take insufficient measures or even no measures at all to protect themselves against cybercrime, which is mainly explained by the lack of awareness, adequately trained staff, or sufficient financial resources. Such observations were also made by (Norris et al., 2020). The analysis of the responses obtained indicate that the reason for such negligence is, above all, the lack of awareness of threats related to the increasingly widespread use of cyberspace and the resulting new tasks and duties that local government units should undertake. The above was reflected in the fact that some respondents indicated that their municipal office does not have a cybersecurity policy, partly due to the fact that there was no electronic document circulation system implemented. At the same time, it proves that Polish municipalities are merely at the second, out of the four, stage of digital government evolution mentioned by (Janowski, 2015) and it will take much longer to make cybersecurity a key element of management.

What is necessary is to disseminate knowledge in this regard (Kańduła & Przybylska, 2020) in order to make the entire society aware of the threats posed by cybercrime. The need for such actions is also highlighted by (de Bruijn & Janssen, 2017).

Research shows that there is a correlation between a lack of security policy and a lack of financial resources. This relationship was also observed by (Hatcher et al., 2020; Norris et al., 2020). Therefore, it is also crucial to disseminate knowledge about available sources of funding for expenses on cybersecurity, and about good practices in this area, as well as to simplify the rules for using external sources of funding, including EU funds. In Poland, EU funds are disbursed based on the Digital Poland Operational Programme 2014-2020, but municipalities have restricted access to these funds, as the programme was designed mainly for state (central) administration units. As a result, 87% of local government offices in Poland have to finance investments in infrastructure protecting against cyber-attacks from their own funds (*Jak to Jest z Cyberbezpieczeństwem w Samorządach?*, 2015).

Only in half of the municipalities surveyed had all office staff trained in the field of cybersecurity, while 9% of the municipalities conducted such training only for managerial staff. The remaining municipalities conduct no training in this regard, excused as financial difficulties. A short-term remedy for this problem might be free training and conferences organised by state entities, as well as the provision of information materials on cybersecurity (KPRM, 2021). In the long run, this problem could be solved by including cybersecurity in the daily management practice of local government units by providing adequate training for future managers and public officials in terms of ICT and cybersecurity issues, as suggested by (Hatcher et al., 2020). The costs of such training could also be covered by EU funds.

5 Conclusions

Ensuring cybersecurity in municipalities is important not only due to legal requirements in this respect, but – above all – in order to guarantee confidentiality, integrity, availability, and authenticity of resources processed in IT systems used to perform public tasks. The tasks of local government units in the field of cybersecurity are beyond the human, organisational, and financial capacity of individual municipalities. There is no doubt that cooperation and exchange of experience in the field of cybersecurity between municipal offices and their organisational units are crucial. The first stage of such cooperation should be a diagnosis of the state of digital security of local government units in order to prepare appropriate procedures and programmes.

The results of this research indicate that increasing the level of cybersecurity among municipalities in Poland requires not only greater financial resources, but also more competent employees, better equipment, and software. These results are very much in line with the research conducted by (Lohrmann, 2019). What is also necessary is to spread awareness of potential risks among officials, develop clear cybersecurity policy standards and procedures, and ensure strict law enforcement.

One possible way to ensure data security is to cooperate with external security auditors and ICT specialists in order to assess the risk of cyber-attacks. This has been suggested by (Hatcher et al., 2020; Norris et al., 2019). Another way to ensure greater data security is to form partnerships with neighbouring municipalities to share knowledge, expenses, and reduce costs. A good solution may also be to use cloud computing services provided by certified, government-tested providers. Such cooperation will help local governments with limited resources to create effective cybersecurity policies (Hatcher et al., 2020).

Restricting the autonomy of municipalities and excessive interference on the part of state authorities in their functioning are not desirable, but given that cybersecurity is a public good (Taddeo, 2019) and economies of scale can be used to provide it, state authorities should carry out random audits to identify any irregularities in this regard (although punitive measures should not be used in case of their detection), as well as help eliminate them and make the system more fault-proof. Education is of key importance not only to show the weaknesses of municipalities, but also to disseminate good practices related to cybersecurity.

The presented survey is the first nationwide survey of municipalities regarding cybersecurity. The research on the approach of Polish municipalities to this issue offers a contribution to the field of economics and management of the public finance sector, both at the national level and European level. Cybercrime poses a threat not only to the function of municipalities, but also to the function of the whole state and individual citizens. The research results provide insights into the state of cybersecurity in Polish municipalities and their ability to counteract security-related incidents, allowing for a better understanding of the problems faced by these units. Therefore, they can be the basis for dissemination of good practices, which will help local authorities prepare for possible attacks. They can also serve as a starting point for further research, prompt changes in legislation, and encourage undertaking actions by the state aimed at raising awareness of cyber-attacks and prepare municipalities to counter them.

Acknowledgement:
The project financed within the Regional Initiative for Excellence programme of the Minister of Science and Higher Education of Poland, years 2019-2022, grant no. 004/RID/2018/19, financing 3,000,000 PLN.

References:

Act of 17 February 2005 on computerization of activities or performing public tasks, *Journal of laws,* 64(565).

Act of 5 July 2018 on the national cybersecurity system, *Journal of Laws,* 1560.

Act of 7 May 2010 on supporting the development of telecommunications networks and services, *Journal of Laws*, 106(675).

Brumfield, C. (2019) *Why local governments are a hot target for cyberattacks* available at: https://www.csoonline.com/article/3391589/why-local-governments-are-a-hot-target-for-cyberattacks.html (November 11, 2021).

Chałubińska-Jentkiewicz, K. (2019) Cyberbezpieczeństwo - kwestie definicyjne, *Cybersecurity and Law*, 2(2), pp. 7-23.

Chałubińska-Jentkiewicz, K. (2021a). Access to the ICT network as a public task of local government, *Lex Localis - Journal of Local Self-Government*, 19(1), pp. 175–195. https://doi.org/10.4335/19.1.175-195(2021)

Chałubińska-Jentkiewicz, K. (2021b) Cybersecurity as a Public Task in Administration., In: Chałubińska-Jentkiewicz, K., Karpiuk, M. & Kostrubiec, J. (eds) *The Legal Status of Public Entities in the Field of Cybersecurity in Poland* (Maribor: Institute for Local Self-Government Maribor), pp. 19–38, https://doi.org/10.4335/2021.5.

Chałubińska-Jentkiewicz, K. (2021c) Cybersecurity Policy. In K. Chałubińska-Jentkiewicz, In: Karpiuk, M. & Kostrubiec, J. (eds.) *The Legal Status of Public Entities in the Field of Cybersecurity in Poland* (Maribor: Institute for Local Self-Government Maribor), https://doi.org/10.4335/2021.5.

Chatfield, A. T. & Reddick, C. G. (2019) A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government, *Government Information Quarterly,* 36(2), pp. 346–357, https://doi.org/10.1016/j.giq.2018.09.007.

D'Agostino, M., Schwester, R., Carrizales, T. & Melitski, J. (2011) A Study of E-Government and E-Governance: An Empirical Examination of Municipal Websites, *Public Administration Quarterly*, 35(1), pp. 3-25.

de Bruijn, H. & Janssen, M. (2017) Building Cybersecurity Awareness: The need for evidence-based framing strategies, *Government Information Quarterly,* 34(1), pp. 1–7, https://doi.org/10.1016/j.giq.2017.02.007.

DiNapoli, T. P. (2016) *comptroller Protecting Sensitive Data and Other Local Government Assets:* (Issue June), available at: https://www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf (November 11, 2021).

Eisenstein, L. (2019) *Why Municipalities Should Care About Cybersecurity,* available at: https://insights.diligent.com/cybersecurity-local-government/why-municipalities-care-cybersecurity (November 11, 2021).

Finster, S. & Baumgart, I. (2015). Privacy-aware smart metering: A survey, *Privacy-Aware Smart Metering: A Survey,* 7(2), pp., 1088–1101, https://doi.org/10.1109/COMST.2015.2425958.

Fusi, F. & Feeney, M. K. (2018) Electronic monitoring in public organizations: Evidence from USIbr local governments, *Public Management Review*, 20(10), pp. 1465–1489, https://doi.org/doi:10.1080/14719037.2017.1400584.

García Zaballos, A. & González Herranz, F. (2013) *From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation* (Issue September), available at: https://publications.iadb.org/publications/english/document/From-Cybersecurity-to-Cybercrime-A-Framework-for-Analysis-and-Implementation.pdf (November 11, 2021).

Grossmann, T., Knopkiewicz, W., Sebzda-Załuska, J., Szydło, M. & Wilczewski, J. (2013) *Ustawa o wspieraniu rozwoju usług i sieci telekomunikacyjnych Komentarz* (Warsaw: C.H. Beck).

Hatcher, W., Meares, W. L. & Heslen, J. (2020) The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices, *Journal of Cyber Policy*, 5(2), pp. 302–325, https://doi.org/10.1080/23738871.2020.1792956.

Heeringa, S. G., West, B. T. & Berglund, P. A. (2017) *Applied Survey Data Analysis*, Chapman and Hall/CRC, https://doi.org/https://doi.org/10.1201/9781315153278.

Ibrahim, A., Valli, C., McAteer, I. & Chaudhry, J. (2018) A security review of local government using NIST CSF: A case study, *The Journal of Supercomputing*, 74, pp. 5171–5186, https://doi.org/doi:10.1007/s11227-018-2479-2.

Polska Szerokopasmowa (2015) *Jak to jest z cyberbezpieczeństwem w samorządach?*, https://www.polskaszerokopasmowa.pl/technologie/artykuly/klucz,jak-to-jest-z-cyberbezpieczenstwem-w-samorzadach,akcja,pdf.html (November 11, 2021).

Janowski, T. (2015) Digital government evolution: From transformation to contextualization, *Government Information Quarterly,* 32(3), pp. 221–236, https://doi.org/doi:10.1016/j.giq.2015.07.001.

Kańduła, S. & Przybylska, J. (2020). Cybersecurity in local government: Essence, tasks and threats, *Digital Transformation of the Financial Sector of Economy*, pp. 45–46, available at: https://www.researchgate.net/publication/344172548_Cybersecurity_in_local_government_Essence_tasks_and_threats (November 11, 2021).

Karpiuk, M. (2021a) Organisation of the National System of Cybersecurity: Selected Issues, *Studia Iuridica Lublinensia,* 30(2), pp. 233–244, https://doi.org/10.17951/sil.2021.30.2.233-244.

Karpiuk, M. (2021b) The Local Government's Position in the Polish Cybersecurity System, *Lex Localis – Journal of Local Self-Government,* 19(3), pp. 609–620, https://doi.org/https://doi.org/10.4335/19.3.609-620(2021).

Karpiuk, M. (2021c) The Tasks of Public Entities within the National Cybersecurity System, In: Chałubińska-Jentkiewicz, K., Karpiuk, M. & Kostrubiec, J. (eds) *The Legal Status of Public Entities in the Field of Cybersecurity in Poland* (Maribor: Institute for Local Self-Government Maribor), pp. 39–48, https://doi.org/10.4335/2021.5.

Kesan, J. P. & Zhang, L. (2019) An empirical investigation of the relationship between local government budgets, IT expenditures, and cyber losses, *IEEE Transactions on Emerging Topics in Computing*, https://doi.org/doi: 10.1109/TETC.2019.2915098.

KnowBe4 (2020) *The Economic Impact of Cyber Attacks on Municipalities*, available at: https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf (November 11, 2021).

Kostrubiec, J. (2021a) Public Entities within the National Cybersecurity System and their Responsibilities, In: Chałubińska-Jentkiewicz, K., Karpiuk, M. & Kostrubiec, J. (eds) *The Legal Status of Public Entities in the Field of Cybersecurity in Poland* (Maribor: Institute for Local Self-Government Maribor), https://doi.org/10.4335/2021.5.

Kostrubiec, J. (2021b) 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,* 19(1), pp. 111–129, https://doi.org/10.4335/19.1.111-129(2021).

KPRM (2021) #*CyberbezpiecznySamorząd*, available at: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczny-samorzad (November 11, 2021).

Lisiak-Felicka, D. & Pytko, M. (2017) Cyberbezpieczeństwo urzędów gmin w województwie łódzkim, *Przedsiębiorczość i Zarządzanie*, 18(4), pp. 439–451, http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ekon-element-000171470341 (November 11, 2021).

Lohrmann, D. (2019) *How Local Governments Can Address Cybersecurity Challenges*, available at: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-local-governments-can-address-cybersecurity.html (November 11, 2021).

Macmanus, S. A., Caruson, K. & McPhee, B. D. (2013) Cybersecurity at the Local Government Level: Balancing Demands for Transparency and Privacy Rights, *Journal of Urban Affairs*, 35(4), pp. 451–470, available at: https://doi.org/10.1111/j.1467-9906.2012.00640.x .

Nemet, G. F. (2009) Demand-pull, technology-push, and government-led incentives for non-incremental technical change, *Research Policy*, 38(5), pp. 700–709, https://doi.org/10.1016/j.respol.2009.01.004.

NIK (2019) *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego* (Warszawa: Nik), available at: https://www.nik.gov.pl/kontrole/P/18/006/ (November 21, 2021).

Norris, D. F., Mateczun, L., Joshi, A. & Finin, T. (2019) Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity, *Public Administration Review*, 79(6), pp. 895–904, https://doi.org/https://doi.org/10.1111/puar.13028.

Norris, D. F., Mateczun, L., Joshi, A. & Finin, T. (2020) Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity, *Journal of Urban Affairs*, 43(8), pp. 1173-1195, https://doi.org/https://doi.org/10.1080/07352166.2020.1727295.

Peters, M., Schneider, M., Griesshaber, T. & Hoffmann, V. H. (2012) The impact of technology-push and demand-pull policies on technical change – Does the locus of policies matter?, *Research Policy*, 41(8), pp. 1296–1308, https://doi.org/10.1016/j.respol.2012.02.004.

Urząd m. st. Warszawy (2020) *Polityka cyfrowej transformacji Miasta Stołecznego Warszawy*, available at: https://um.warszawa.pl/waw/strategia/polityka-cyfrowej-transformacji (October 15, 2020).

Reddick, C. G. (2004) A two-stage model of e-government growth: Theories and empirical evidence for U.S. cities, *Government Information Quarterly*, 21(1), pp. 51–64, https://doi.org/https://doi.org/10.1016/S0740-624X(99)80003-3.

Regulation of 12 April 2012 on the National Interoperability Framework, minimum requirements for public registers and the exchange of information in electronic form, and minimum requirements for ICT systems, *Journal of Laws*, 526.

Regulation of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Journal of Laws*, 679.

Ruohonen, J. (2020). An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union, *European Journal for Security Research*, 5(2), pp. 349–377, https://doi.org/10.1007/s41125-019-00053-w.

Salminen, M. & Hossain, K. (2018) Digitalisation and human security dimensions in cybersecurity: An appraisal for the European High North, *Polar Record*, 54(2), pp. 108–118, https://doi.org/10.1017/S0032247418000268.

Schallbruch, M. & Skierka, I. (2018) *Cybersecurity in Germany By Martin Schallbruch and Isabel Skierka*, Digital Society Institute, https://doi.org/10.1007/978-3-319-90014-8.

Świtała, K. (2019) Obowiązki jednostek samorządu terytorialnego w Krajowym Systemie Cyberbezpieczeństwa, In: Czaplicki, K., Gryszczyńska, A. & Szpor, G. (eds) *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (Warsaw: Wolters Kluwer).

Szabó, Z. (2019) The Effects of Globalization and Cyber Security on Smart Cities, *Interdisciplinary Description of Complex Systems*, 17(3), pp. 503–510, https://doi.org/10.7906/indecs.17.3.10.

Taddeo, M. (2019) Is Cybersecurity a Public Good?, *Minds and Machines*, 29(3), pp. 349–354, https://doi.org/10.1007/s11023-019-09507-5.

Wojciechowska-Filipek, S. & Ciekanowski, Z. (2019) *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki – organizacji – państwa*. (Warszawa: CeDeWu Sp. z o. o.).

Wolff, J. & Lehr, W. (2018) When cyber threats loom, what can state and local governments do?, *Georgetown Journal of International Affairs*, 19, pp. 67–75, https://doi.org/doi:10.1353/gia.2018.0008.

Zhao, J. J. & Zhao, S. Y. (2010) Opportunities and threats: A security assessment of state e-government websites, *Government Information Quarterly*, 27(1), pp. 49–56, https://doi.org/doi:10.1016/j.giq.2009.07.004.

Tables

Table 1: Characteristics of examined municipalities in terms of their location, population and revenue per capita.

	Number	Percent		Number	Percent
Province			**Number of residents**		
Warmińsko-mazurskie	86	4.8%	Up to 10 000	1150	64.4%
Wielkopolskie	6	0.3%	10 000-20 000	373	20.9%
Dolnośląskie	121	6.8%	20 000-30 000	109	6.1%
Kujawsko-pomorskie	125	7.0%	30 000-40 000	47	2.6%
Lubelskie	152	8.5%	40 000-50 000	34	1.9%
Lubuskie	64	3.6%	50 000-100 000	38	2.1%
Łódzkie	143	8.0%	Over 100 000	36	2.0%
Małopolskie	161	9.0%			
Mazowieckie	241	13.5%	**Revenue per capita**		
Opolskie	56	3.1%	Less than 3 000	652	36.5%
Podkarpackie	114	6.4%	3 000-3 500	182	10.2%
Podlaskie	99	5.5%	3 500-4 000	231	12.9%
Pomorskie	95	5.3%	4 000-4 500	324	18.1%
Śląskie	151	8.4%	4 500-5 000	213	11.9%
Świętokrzyskie	76	4.3%	Over 5 000	185	10.4%
Zachodniopomorskie	97	5.4%			

Source: Own elaboration based on research.

Table 2: Implementation of information security management systems in municipalities.

	Number	Percentage		Number	Percentage
Has the municipality been recognised as a key service operator?			**Why has the municipality not implemented an information security management system?**		
Yes	64	3.6%	Lack of sufficient financial resources	155	37.5%
No	1723	96.4%	Lack of electronic document circulation system	103	24.9%
Who has been appointed to contact the national security system entities?			Nobody – no obligation to do so	83	20.1%
Mayor or deputy mayor	26	40.6%	The municipality does not have an IT specialist	15	3.6%
Municipal secretary	6	9.4%	Nobody – no need to do so	26	6.3%
IT specialist	26	40.6%	Other reason	31	7.5%
Other person	6	9.4%			
Has an information security management system been implemented in the office?			**The municipality would consider implementing an information security management system if:**		
Yes	1374	76.9%	Government administration provided subsidies for this purpose	216	52.3%
No	413	23.1%	An electronic document circulation system was implemented	81	19.6%
Is the implemented information security management system accredited for compliance with the PN-ISO/IEC 27001:2014 standard?			The municipality received co-financing from EU funds	54	13.1%
Yes	244	17.8%	The municipality will sign an agreement with neighbouring municipalities to jointly implement such a system	11	2.7%
No	1130	82.2%	In other cases	51	12.3%

Source: Own elaboration based on research.

Table 3: Information security assessment in municipalities.

	Number	Percentage		Number	Percentage
Do you regard cybercrime as a threat to the municipal office?			**Does the office conduct an internal information security audit on an annual basis?**		
I don’t know	91	5.1%	No	447	25.0%
No threat	63	3.5%	Yes, by an internal auditor	538	30.1%
Minimal threat	259	14.5%	Yes, by an external service provider	802	44.9%
Medium threat	624	34.9%	**Why does the municipal office not carry out an internal information security audit?**		
Significant threat	561	31.4%	No obligation to do so	140	31.3%
Major threat	189	10.6%	No financial resources	265	59.3%
Does the office conduct a regular analysis of the risk of loss of integrity, confidentiality and availability of information?			Other reasons	42	9.4%
Yes	1402	78.5%	**Did any incidents related to information security breaches occur in the office between 2017 and 2019?**		
No	385	21.5%	No	1550	86.7%
Why is no analysis of the risk of loss of integrity, confidentiality and availability of information carried out in the office?			Yes, up to 5 incidents	190	10.6%
No obligation to do so	95	24.7%	Yes, up to 10 incidents	19	1.1%
No financial resources	137	35.6%	Yes, up to 20 incidents	7	0.4%
No employee assigned with such duties	62	16.1%	Yes, more than 20 incidents	21	1.2%
Lack of employees with required skills	73	19.0%	**Has the information security incident been reported?**		
Other reasons	18	4.7%	No	118	44.4%
Does the office maintain an up-to-date and comprehensive electronic record of IT equipment?			Yes – to the police	50	18.8%
Yes	1447	81.0%	Yes – at cert.pl or cert.gov.pl	54	20.3%
No	340	19.0%	Yes – other	44	16.5%

Source: Own elaboration based on research.

Table 4: Areas susceptible to cybercrime, types of cybercrime and security solutions used in municipal offices.

	Number	Percent		Number	Percent
Indicate the areas of your office that you believe are particularly vulnerable to cybercrime?			**Which of the following solutions are implemented in your office?**		
Critical infrastructure	301	16.8%	Firewall	1591	89.0%
Cloud infrastructure	145	8.1%	Antivirus software	1720	96.3%
Personal data	967	54.1%	Vulnerability scanners	294	16.5%
Online services/web applications/websites	593	33.2%	Spam blockers and filters	1237	69.2%
Payment systems	347	19.4%	Data encryption	992	55.5%
Employees	1028	57.5%	Early warning systems	139	7.8%
Workstations (employee equipment)	787	44.0%	VOIP encryption	97	5.4%
Other	45	2.5%	Dedicated VPN resources	627	35.1%
Indicate types of cybercriminal activity that have occurred in your office:			SIEM (Security Information and Event Management)	49	2.7%
Phishing	474	26.5%	IDS/IPS systems (intrusion detection)	644	36.0%
Spam	1413	79.1%	DLP systems (data leakage protection)	184	10.3%
Information leakage	54	3.0%	Other	78	4.4%
Botnet	28	1.6%			
Malware	474	26.5%			
Code injection	26	1.5%			
Data theft (disclosure of confidential information)	19	1.1%			
Rogueware/ransomware/scareware	143	8.0%			
Drive-by-download on infected website	62	3.5%			
Other	211	11.8%			

Source: Own elaboration based on research.

Table 5: Cybersecurity management.

	Number	**Percentage**		**Number**	**Percentage**
How is cybersecurity managed in your office?			**Why has cybersecurity training not been conducted in your office?**		
Internally (employee(s) appointed to manage security policy)	1579	88.4%	No obligation to do so	277	38.2%
Through Internet Service Provider (IPS)	262	14.7%	No financial resources	394	54.3%
Outsourcing – specialist/external company	431	24.1%	Other	54	7.4%
Other	27	1.5%	**Is the municipality insured against the risk of cyber-attack?**		
Was cybersecurity training conducted for the employees of the municipal office between 2017 and 2019?			Yes, the insurance policy covers this risk	204	11.4%
No	725	40.6%	No, but purchasing such insurance is considered	956	53.5%
Yes, for managerial staff	160	9.0%	No, there is no need to do so	627	35.1%

Source: Own elaboration based on research.

Table 6: Results of Pearson's χ2 test analyses for the correlation between the perception of cybersecurity threats to the office and actions undertaken to reduce them.

Do you regard cybercrime as a threat to the municipal office?	χ^2	*df*	*p*	*V*
Has an information security management system been implemented in the office?	0.31	2	.857	.01
Does the office conduct a regular analysis of the risk of loss of integrity, confidentiality and availability of information?	14.66	2	.001	.09
Does the office maintain an up-to-date and comprehensive electronic record of IT equipment?	3.15	2	.207	.04
Does the office conduct an internal information security audit on an annual basis?	6.39	4	.172	.04
Was cybersecurity training conducted for the employees of the municipal office between 2017 and 2019?	9.75	4	.045	.05

χ^2- Chi-square statistic, *df*- degrees of freedom, *p*- statistical significance, *V*- Cramer's V strength of correlation.
Source: Own elaboration based on research.

Table 7: Results of Pearson's χ^2 tests for the correlation between the implementation of an information security management system and the occurrence of security breaches.

Has an information security management system been implemented in the office?	χ^2	*df*	*p*	*V*
Did any incidents related to information security breaches occur in the office between 2017 and 2019?	4.28	4	.369	.05
Types of cybercriminal activity that have occurred in your office:				
Phishing	0.48	1	.488	.02
Spam	0.59	1	.443	.02
Information leakage	4.51	1	.034	.05
Botnet	1.25	1	.264	.03
Malware	1.47	1	.225	.03
Code injection	0.22	1	.636	.01
Data theft (disclosure of confidential information)	0.05	1	.831	.01
Rogueware/ransomware/scareware	0.70	1	.402	.02
Drive-by-download on infected website	0.17	1	.684	.01
Other	3.17	1	.075	.04

χ^2- Chi-square statistic, *df*- degrees of freedom, *p*- statistical significance, *V*- Cramer's V strength of correlation.
Source: Own elaboration based on research.

Table 8: Results of Pearson's χ^2 tests for the correlation between conducting periodic analyses of the risk of loss of integrity, confidentiality, and availability of information and the occurrence of security breaches.

Does the office conduct a regular analysis of the risk of loss of integrity, confidentiality and availability of information?	χ^2	*df*	*p*	*V*
Did any incidents related to information security breaches occur in the office between 2017 and 2019?	10.41	4	.034	.08
Types of cybercriminal activity that have occurred in your office:				
Phishing	5.58	1	.018	.06
Spam	5.40	1	.020	.06
Information leakage	3.59	1	.058	.05
Botnet	0.89	1	.346	.02
Malware	7.58	1	.006	.07
Code injection	1.56	1	.211	.03
Data theft (disclosure of confidential information)	1.38	1	.240	.03
Rogueware/ransomware/scareware	0.65	1	.419	.02
Drive-by-download on infected website	1.11	1	.291	.03
Other	5.00	1	.025	.05

χ^2- Chi-square statistic, *df*- degrees of freedom, *p*- statistical significance, *V*- Cramer's V strength of correlation.
Source: Own elaboration based on research.