SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 221

INFORMATION SECURITY INCIDENT MANAGEMENT AND CYBERSECURITY AWARENESS IN LOCAL GOVERNMENT IN POLAND

Dominika LISIAK-FELICKA[1*], Maciej SZMIT[2]

[1] Department of Economic and Medical Informatics, Faculty of Economics and Sociology, University of Lodz; dominika.lisiak@uni.lodz.pl, ORCID: 0000-0001-8451-4268
[2] Department of Computer Science, Faculty of Management, University of Lodz; maciej.szmit@uni.lodz.pl, ORCID: 0000-0002-6115-9213
* Correspondence author

Purpose: The aim of this article was to examine and diagnose the existing situation in the field of information security management in local government offices in Poland. The focus was on the following issues: information security incident management, training, security level assessment, and financial aspects.
Design/methodology/approach: The survey has exploratory character. It was conducted using the CAWI technique based on the online questionnaire which was sent to all offices of local government units: marshal offices, district offices and municipality offices.
Findings: The text presents some of the survey results on information security awareness and information security incidents conducted in 2023 in local administration offices in Poland, especially about the numbers of information security incidents, training, budgets allocated on information security management, and assessment of security levels. The research results provide knowledge about the existing situation in the field of information security management in local government administration in Poland.
Research limitations/implications: There are certain limitations to the use of survey research. The low level of participation means that the results may not be representative of the population. Additionally, respondents may intentionally provide false information or hide certain facts, which affects the reliability of the results.
Practical implications: The presented results provide a valuable knowledge base on cybersecurity management in local government offices and can be the basis for further research and analysis.
Originality/value: To the authors' knowledge, this type of research has not been conducted. The research results provide knowledge about the existing situation in the field of information security management in local government administration in Poland. Information security incident management is one of the elements necessary for the proper operation of Information Security Management Systems.
Keywords: information security, information security incidents, cybersecurity awareness, local administration.
Category of the paper: research paper.

1. Introduction

Information security management issues, from the management point of view, belong to the area of GRC (Governance, Risk Management and Compliance). A particularly important regulation in this context is the General Data Protection Regulation (GDPR), which imposes numerous obligations on local administration offices, in regard to having an Information Security Management System (ISMS) and reporting incidents related to personal data security breaches.

An information security incident has been defined in the standard ISO/IEC 27000:2018-3.31 as a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. A similar definition can be found in the standard ISO/IEC 27002:2022-3.1.15 information security incident – one or multiple related and identified information security events that can harm an organization's assets or compromise its operations.

The same standards define information security incident management as a set of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents (PN-ISO/IEC 27000:2018-3.32) and as an exercise of a consistent and effective approach to the handling of information security incidents (ISO/IEC 27002:2022-3.1.16).

It should be noted that incident management is not only a set of actions and procedures enabling effective response to incidents, but also minimizing their effects and preventing their occurrence in the future. Information security incident management is one of the key elements of Information Security Management Systems (Lisiak-Felicka, 2024).

To properly manage an incident, it is, of course, necessary to both detect the security breach (the earlier, the better) and respond appropriately, both on the part of appropriate specialists (Digital Evidence First Responders) and employees of the organization that fall victim to the incident. Appropriate response to information security events is one of the issues covered by information security awareness.

The article focuses on cybersecurity issues in local government units. Importantly, cybersecurity is one of the key aspects of the functioning of local government offices. These institutions store and process huge amounts of data, such as citizens' personal information, financial information or strategic documents. The security of this data is therefore directly related to the security of citizens. Local government offices are obligated to comply with data protection regulations, such as the GDPR. A breach of data security can lead to identity theft, financial abuse and loss of public trust.

Every now and then and again the media reports cases of ransomware or other attacks directed towards the public administration in Poland. These incidents can paralyze the functioning of the office by blocking access to IT systems (see. e.g. Klimczuk (2024a, 2024b),

Makowiec (2024)). Such incidents can require expensive data recovery and cause delays in providing services to citizens.

Cyber criminals' activity also has an influence on the continuity of office operations. The functioning of local government administration is crucial to ensuring residents have access to basic services. In the event of a serious incident affecting an IT system, services may be interrupted, and citizens may lose access to offices' services.

Local governments often manage critical infrastructure, such as water supply, transportation systems, or energy systems. A cyberattack on such systems can have serious consequences for the local community (Banasik, Bagińska, 2019).

Failure to ensure an adequate level of cybersecurity can lead to a loss of trust in public institutions. Therefore, local government offices should invest in modern security systems, regular employee training to effectively protect data and ensure the continuity of their operations and services.

Cybersecurity Department in the Polish Ministry of Digital Affairs prepared a set of recommendations standardizing security solutions in networks and information systems (called the National Cybersecurity Standards (NSC)), based on the US National Institute Standard and Technology's documents. Given both their optional nature and the problems with information security management in local administration made apparent by the Supreme Audit Office's report (NIK, 2018), it seems interesting how local government in Poland deal presently with Information Security issues, so the aim of the research was to analyse the existing situation in the field of information security incident management in these offices.

To the authors' knowledge no in-depth diagnostic studies on the incident management in local government offices have been conducted.

2. Literature review

The issue of information security management in public administration has not been researched extensively. Typically, researchers focus on different types of organizations, enterprises, and economic sectors. In the article (Wenlong et al., 2023), the authors conducted a systematic review of the literature (including 380 English-language items from the Web of Science, Scopus, IEEE, ACM, ScienceDirect, SAGE, Oxford Academic and Google Scholar databases) devoted to empirical research on the effectiveness of the GDPR using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analysis) approach. One of the conclusions of this review is that the literature on the GDPR in the public sector is sparse: the authors found only two articles: one regarding Poland (Lisiak-Felicka, Szmit, 2021a, pp. 1-21) and one – Czech Republic (Faifr, Januška, 2021, pp. 1124-1141). Although there are also a few other studies on ISMS and/or information security aspects of the GDPR in public

administration in other countries, such as Martins et al. (2020, pp. 205-216), Oliveira, Dias (2023), or Starčevič et al. (2018, pp 163-176). Only rare articles are devoted to cases in local administration Homburg, Kokje (2020, pp. 211-218), Ali et al., (2020), Marcut (2018, p. 337) or Lisiak-Felicka et al. (2022, pp. 382-394) and there are also several articles published in national languages (e.g., in Polish: Jatkiewicz (2015) or Chodakowska et al. (pp. 129-148).

Obviously the GDPR-related issues do not exhaust the subject of information security, but even precisely determining the number of publications devoted to this topic may be difficult. One of the reasons is the lack of uniform terminology regarding information security. There are many terms used sometimes as synonyms, and sometimes with different meanings (e.g. information security, information safety, data security, data safety, cybersecurity, cybersafety). The term 'local administration' can also refer to various types of offices depending on the system of government in a particular country. Additionally, the terms 'local government', 'local administration', 'municipality', 'civic government' etc. are sometimes used. There is another systematic literature review based on the PRISMA protocol concerning the keywords 'cybersecurity', 'cyber threat', 'cyber risk', 'local government', 'municipality', 'council', and 'smart city' in the article (Hossain et al., 2025). The Authors identified 3861 records as result of the query: (articles titles, abstract, keyword contains: ((“cybersecurity” OR “cyberthreat” OR “cyber risk” OR “information security” OR “data security”) AND (“smart city” OR “local government” OR “municipality” OR “council”)) from Scopus, ScienceDirect, Directory of Open Access Journal, Wiley Online Library and QUT Library Collection and after two stages of the screening process (excluding books, chapters etc. and excluding articles not in English in the first stage and excluding papers irrelevant to the research aim in the second stage) only 123 papers were left.

In a different article (Vestad, Yang, 2023) the systematic review based on the query: (“municipal” OR “municipality”) AND “cybersecurity” was conducted and original search result that consisted of 627 papers and after title screening and abstract screening only 34 papers were left. The Authors distinguished 7 article topics: Smart Cities, Operational Technology, Elections, Human Issues and Cybersecurity Awareness, Crisis Management, Management and Governance and Municipal Technology (use of secure protocols and certificates by municipalities).

Comparing the number of articles focused on information security and local administration with the number of articles dedicated to information security management in general, even without conducting a systematic literature review, it is evident that the number of the former is one or even two orders of magnitude smaller (Table 1).

It seems that administration information security issues deserve more attention, especially considering the current situation of war beyond Poland's eastern border. According to the Microsoft Threat Intelligence report published in 2023 (Microsoft, 2023) government, including local government institutions, are the most common target of attacks by

cybercriminals and Poland is the second most frequent target of cybercriminals after the USA (not counting Ukraine).

Table 1.
Number of publications devoted to information security management and information security and local government

	"Information security" AND "management"	"Cyber security" AND "management"	"Information security" AND "local government"	"Data security" AND "local government"	"Information security" AND "local administration"	"Data security" AND "local administration"	"Cyber security" AND "local government"	"Cyber security" AND "local administration"
Web of Science Core Collection (All fields)	9482	3476	31	13	2	0	10	1
Scopus (All fields)	131908	69847	1578	451	35	13	896	16
Science Direct	22515	10942	895	925	44	46	496	24
IEEE	14311	10979	1127	929	456	444	220	63
ACM	6711	4060	217	207	17	20	146	13
OpenAlex (Full text)	2182	385	9	1	0	0	1	12
Lens.org	34464	12013	365	342	25	30	167	8

Source: Authors' own study.

Additionally, the constantly increasing number of threats is confirmed by reports prepared by the national computer incident response teams: CERT.PL and CSIRT.GOV.PL (Figure 1 and Figure 2).

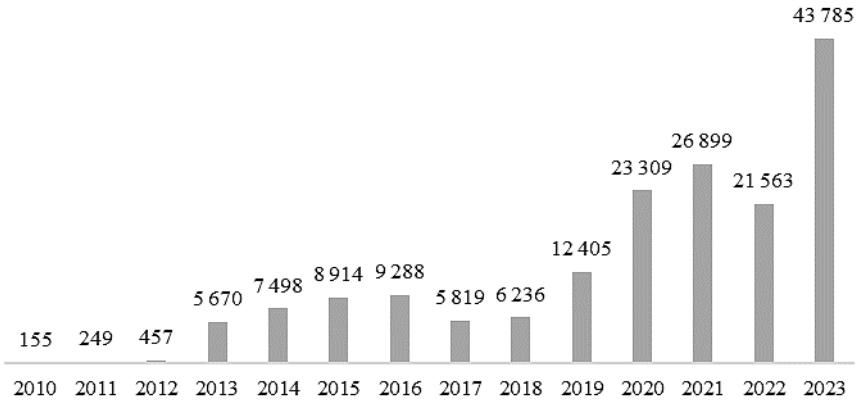


Figure 1. Numbers of incidents reported by CSIRT.GOV.PL.
Source: Authors' own study based on (CSIRT.GOV.PL, 2024).

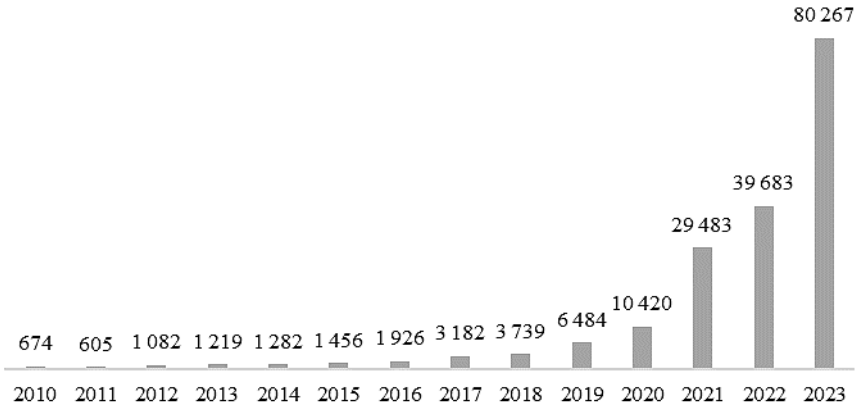


Figure 2. Numbers of incidents reported by CERT.PL.

Source: Authors' own study based on (CERT.PL, 2024).

These teams (CERT.PL and CSIRT.GOV.PL) are responsible for the registration and handling of network security incidents at the national level. The third team CSIRT.MIL also works at national level but it does not publish statistics about the incidents.

3. Research methods

The aim of the study was to analyse the existing situation in the field of information security management, especially incident management, in local government offices in Poland. The focus was on the following issues: information security incident management, training, assessment of a security level and financial aspects.

In social sciences, a survey is most often a tool used to learn about the opinions and positions of respondents. In our research, however, we used it to collect information about the existing state of affairs, primarily because - to our knowledge - no systematic analyses are being conducted on the cybersecurity of local administration. The following research questions were formulated:

- Q1: How many incidents have occurred in years 2020-2022 and where were they reported?
- Q2: Could offices count on support from other state administration bodies in the field of incident management?
- Q3: What were the dominant types of incidents reported and what is the most vulnerable element in the office to attacks by cybercriminals?
- Q4: Were offices providing good training in the field of cybersecurity?
- Q5: How offices assess the level of security and what is an approximate annual budget allocated to cybersecurity?

The survey was conducted using the CAWI (Computer-Assisted Web Interview) technique based on a questionnaire containing 44 questions, developed using Microsoft Forms. The survey was anonymous and was conducted at the turn of July and August 2023. The results of the part of the study devoted to the implementation and operation of information security management systems are presented in the article (Lisiak-Felicka, Szmit, 2023, pp. 400-407).

To conduct the study, e-mails were sent to all offices of local government units: marshal offices, district offices and municipality offices. As of January 1, 2023, Poland was divided into 16 voivodeships, 314 counties and 2477 municipalities (302 urban, including 66 cities with county rights, 677 urban-rural, and 1498 rural (GOV.PL, 2023).

Obtained 236 responses from 2,807 offices: 5 marshal offices, 34 district offices and 197 municipal offices. The distribution of responses was compared with the structure of administrative offices in Poland using Renkonen Similarity Index, Sr, calculated based on the formula (1):

$$S_r = \sum_{1}^{i} \min(p_{1,i}, p_{2,i}) \tag{1}$$

where p is the percentage share of a given fraction.

The calculated value was 0.95, which may be interpreted as very high similarity, therefore the structure of the studied sample was very similar to the structure of the population.

Figure 3 shows the geographical location of the offices participating in the study. Most responses were received from the following voivodeships: Greater Poland, Lesser Poland, Lodz, and Masovian. The visualization does not include the locations of the 5 marshal offices that participated in the study due to the possibility of their identification which would be equivalent to deanonymizing some participants. The survey was anonymous and therefore marshal offices were not asked about their location.

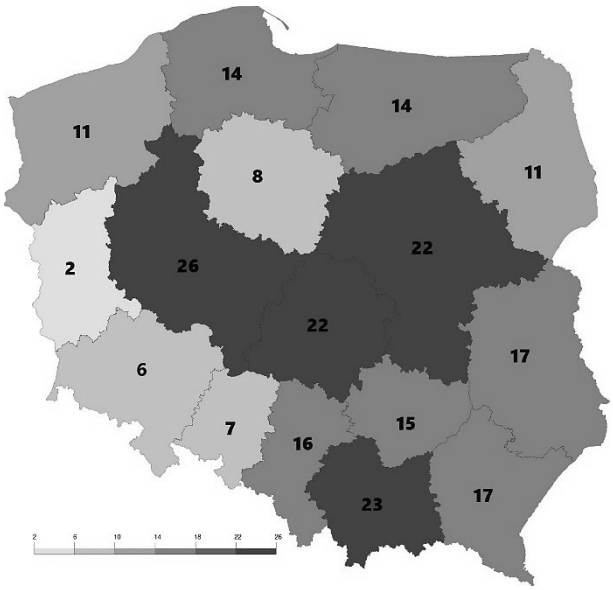


Figure 3. Geographic location of offices participating in the research.

Source: Authors' own study.

It should be noted that survey research is useful for obtaining quantitative data on a large scale, but its effectiveness depends primarily on the involvement of respondents.

4. Results

The results of the study are divided into the following sections: information security incident management, training, security level assessment, and financial aspects.

4.1. Information security incident management

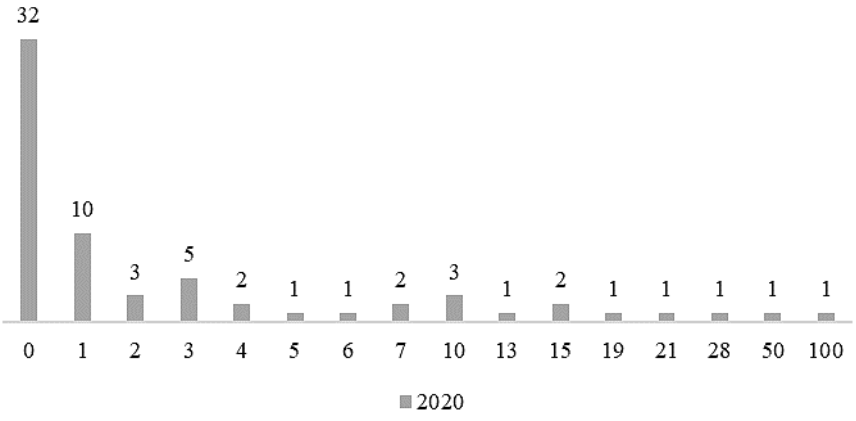
Respondents were asked several questions related to information security incident management. Of the 236 respondents, 78 (33%) confirmed that they had experienced security incidents in the past. There were no such events in most municipal offices. Detailed results are presented in Table 2.

Table 2.
Answers to the question: "Have there been any security incidents in the office in the past?"

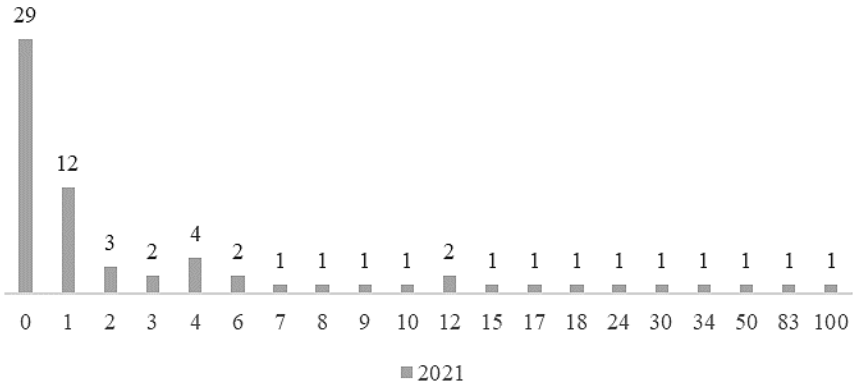
Have there been any security incidents in the office in the past?	Marshal Office	District Office	Municipal Office	Total
yes	4	19	55	78
no	1	15	142	158
Total:	5	34	197	236

Source: Authors' own study.

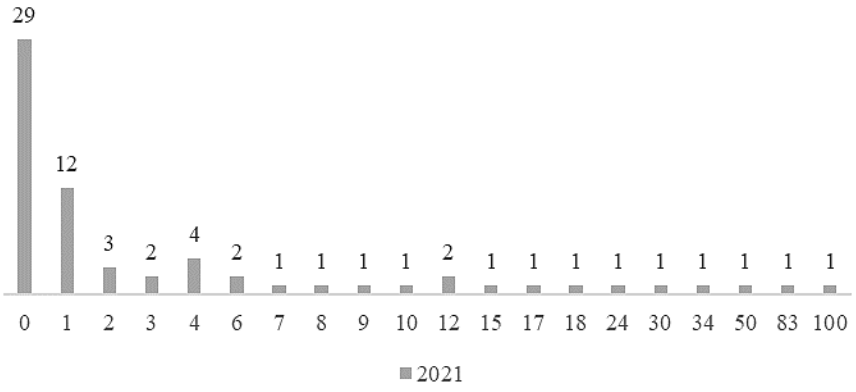
Next question was about the number of security incidents recorded between 2020 and 2022. The results are presented in Figure 4. The dominant numbers of incidents in the examined period were 0 and 1. Two offices refused to answer these questions.



a)



b)



c)

Figure 4. Answers to the question: "How many security incidents were recorded in 2020 (a), 2021 (b) and 2022 (c)?"

Source: Authors' own study.

Of the 78 offices where security incidents have occurred, the vast majority (64) declared that they had reported this fact to CERT, CSIRT, the prosecutor's office, the Personal Data Protection Office, or other appropriate entities.

Half of the offices (39) also declared that they could count on support from other state administration bodies in the field of incident management. This assistance consisted primarily of cooperation with computer incident response teams. In this context, respondents pointed to the help from CERT Polska - CSIRT NASK in terms of sharing knowledge (playbooks, forms for reporting incidents, instructions on how to proceed with reporting an incident, publications on new threats), but also in the ongoing handling of incidents (accepting reports, sending comments and feedback). Below are some of the respondents' opinions about this cooperation:

- "CSIRT NASK - supports local governments during cyberincidents",
- "incident analysis by CERT, possible technical assistance in the event of a security incident",
- "assistance only from CSIRT NASK - assistance in incident analysis, recommendations, good practices, working meetings, evidence analysis, etc.",

- "after submitting a report to CSIRT NASK, we receive support from operators who conduct post-intrusion analysis",
- "substantive and technical assistance of the CSIRT NASK team during the analysis and response to the incident",
- "in connection with the notification to CSIRT NASK, we received a quick response dispelling our doubts",
- "CERT publishes messages about attacks on its websites. There is also a special application for information security coordinators, but it does not work well at the moment".

The responses also indicated several advisory support in the field of incident handling, diagnostics, training, incident analysis, taking corrective actions, as well as cooperation with the Personal Data Protection Office in the field of incident reporting forms.

Authorities provided advice when the need for help was reported. Assistance was received in securing evidence, cooperation in the analysis of the effects of incidents or violations, provision of advice and recommendations, provision of incident response procedure and guidelines for further action on the incident, substantive support, exchange of experiences, joint training, common assistance in the development of documentation, training materials of the Chancellery of the Prime Minister and providing the offices with access to national cybersecurity system S46 in 2023 (S46-react is a project of the Research and Academic Computer Network - National Research Institute, which will help raise the level of cyber security and combat cyber threats more effectively).

The next question concerned the elements in the office that, in the respondents' opinion, were most susceptible to attacks by cybercriminals. Respondents unanimously indicated that people (employees) are the weakest link in the security system (Figure 5). In addition to the elements provided in the catalogue, one office also indicated its own answer – "systems available from public addresses".

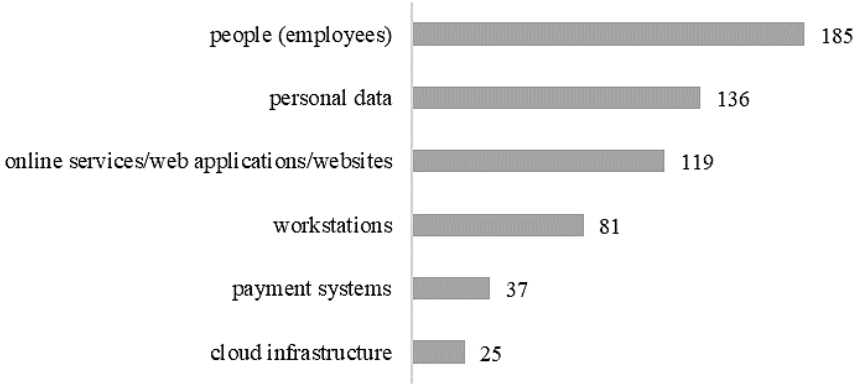


Figure 5. Answers to the question: Which of the following elements in the office do you consider most susceptible to attacks by cybercriminals?"

Source: Authors' own study.

In the next question, respondents indicated the categories of incidents that, in their opinion, constitute the greatest threat to the office. The question uses the CSIRT GOV incident categories:

- Abusive content (e.g., harmful speech, child pornography, violence).
- Malicious code (e.g., virus, trojan, ransomware, dialer, botnet).
- Information gathering (e.g., scanning, sniffing, spam, social engineering).
- Intrusion attempts (e.g., attempts to exploit know vulnerabilities, login attempts).
- Intrusions (e.g., hacking into an account, application, system, infrastructure).
- Availability issues (e.g., DoS, DDoS, sabotage, failure, negligence, technical service work).
- Information content security (e.g., unauthorized access to information, unauthorized modification of information).
- Fraud (e.g., unauthorized use of resources, copyright infringement, impersonation, identity theft, phishing).
- Vulnerable (e.g., misconfiguration, vulnerability detection).
- Cyberterrorism (a terrorist event committed in cyberspace).

The responses are presented in Figure 6. The dominant category in responses is malware.

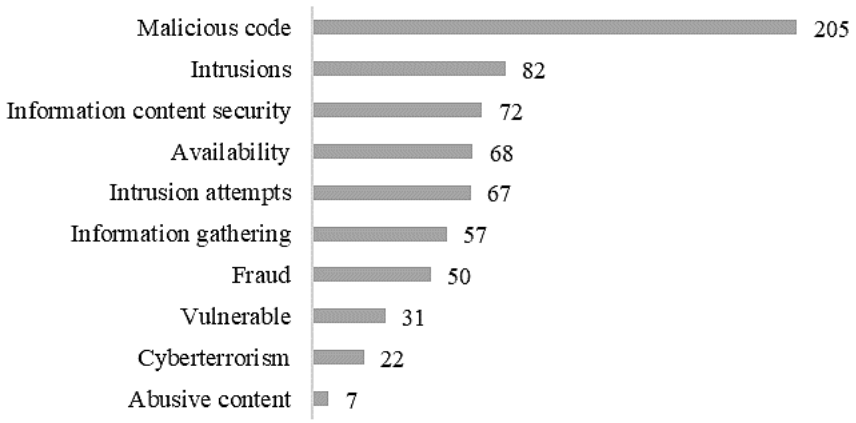


Figure 6. Answers to the question: "Which categories of incidents, in your opinion, pose the greatest threat to the office?"

Source: Authors' own study.

One of the respondents gave his own answer: "unauthorized publication/sharing of data", which, however, can be included in the "information content security" category.

4.2. Training

Respondents were also asked to answer questions related to training conducted for employees in the field of cybersecurity and related subjects. Out of 236 offices, 171 (72%) conducted such training. Table 3 presents data on the number of training courses conducted during the period under study (2020-2022). Based on the data provided by the offices, many offices conduct 1-2 training courses on this subject per year.

Table 3.
Answers to the question: "How many such training courses were organized in 2020, 2021, and 2022?"

	Number of responses		
Number of training courses	**2020**	**2021**	**2022**
1	95	96	106
2	21	25	27
3	2	5	15
4	2	1	2
5	4	2	2
6	0	1	3
7	0	1	2
8	1	2	0
10	0	0	2
14	0	0	1
15	1	0	0
16	1	0	0
20	0	1	0
30	0	0	1
no data	44	37	10

Source: Authors' own study.

The dominant subjects of the training were: cybersecurity, information security and personal data protection. Detailed data are presented in Figure 7.

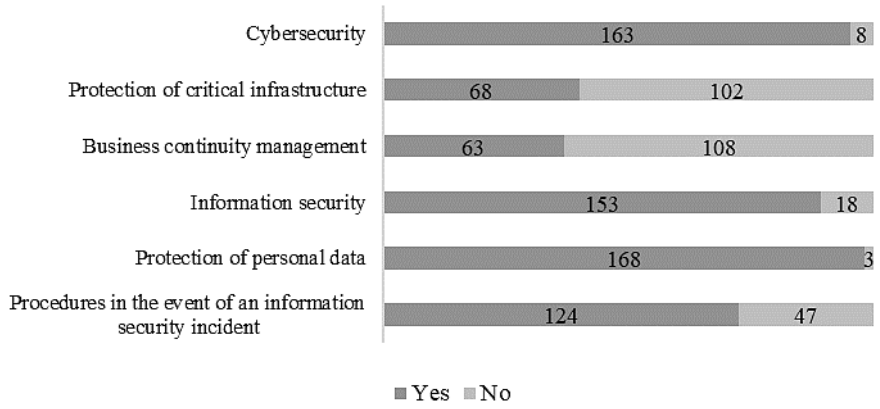


Figure 7. Answers to the question about the scope of training.
Source: Authors' own study.

4.3. Security level assessment and financial aspects

The next question concerned subjective assessment of the level of security in the office on a scale from 1 to 5, where 1 was the lowest and 5 was the highest. Most respondents chose a rating 3 or 4 (Figure 8). Detailed data by type of office is presented in Table 4. The lowest ratings (1 or 2) were only selected by municipal offices.

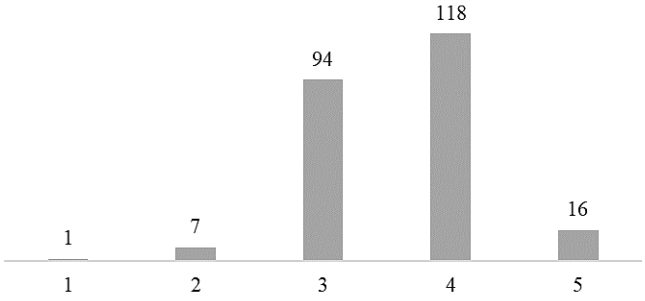


Figure 8. Answers to the question: "On a scale from 1 to 5, how do you rate the level of information security in the office?"

Source: Authors' own study.

Table 4.
Answers to the question: "On a scale from 1 to 5, how do you rate the level of information security in the office?"

Assessment	Marshal Office	District Office	Municipal Office	Total
1	0	0	1	1
2	0	0	7	7
3	0	13	81	94
4	4	16	98	118
5	1	5	10	16
Total	5	34	197	236

Source: Authors' own study.

Out of the 236 surveyed offices, only 8 assessed the level of cybersecurity management maturity in the organization - one district office and 7 municipal offices. When specifying the methodology according to which this assessment was made, 3 offices indicated CMMI (Capability Maturity Model Integration), and the remaining offices indicated their own answers: "other", "according to the methodology used by the Data Protection Inspector", "based on the requirements contained in PN ISO/IEC 27001 and §20 Regulation on the National Interoperability Framework (Regulation of the Council of Ministers), "external audit". One respondent did not answer.

Respondents were also asked to specify the office's indicative annual budget allocated to cybersecurity, including expenses for personal data security. The results are presented in Figure 9. The dominant answer was "less than 10,000 PLN", which means that more than half of the surveyed offices allocate very small amounts for this purpose. Detailed answers to this question broken down by type of office are presented in the Table 5.

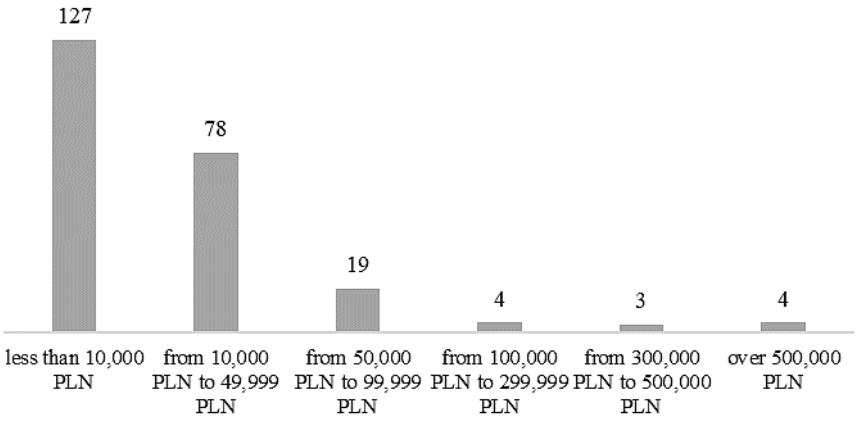


Figure 9. Answers to the question: "What is the office's approximate annual budget allocated to cybersecurity, including expenses for personal data security?"

Source: Authors' own study.

Table 5.
Answers to the question: "What is the office's approximate annual budget allocated to cybersecurity, including expenses for personal data security?"

The office's indicative annual budget for cybersecurity, including expenses for personal data security	Marshal Office	District Office	Municipal Office	Total
less than 10,000 PLN	1	8	118	127
from 10,000 PLN to 49,999 PLN	0	19	59	78
from 50,000 PLN to 99,999 PLN	1	6	12	19
from 100,000 PLN to 299,999 PLN	0	1	3	4
from 300,000 PLN to 500,000 PLN	1	0	2	3
over 500,000 PLN	2	0	2	4

Source: Authors' own study.

The last question concerned the respondents' opinions on the biggest problems in ensuring an appropriate level of cybersecurity in the office (Figure 10). The dominant answer was "lack of sufficient financial resources", which directly corresponds to the previous question.

Figure 10. Answers to the question: "What, in your opinion, is the biggest problem in ensuring an appropriate level of cybersecurity in the office?"

Source: Authors' own study.

Other problems mentioned by the respondents include: “some activities can only be conducted after office hours”, “the Municipal Mayor - the biggest problem”, “imposition of the most malware-riddled operating system by central/superior units”, “insufficient number of employees”, “too few IT staff”. One of the comments did not concern this question and read: “The Municipal Office has an information security policy developed and implemented by itself”. However, one of the respondents stated that “there is never the right level of security”.

5. Discussions

To the best of our knowledge, no comparable surveys of the issues of information security incidents and security awareness in local administration offices in Poland have been published. The above results (hereinafter referred to as survey C) were compared with our previous surveys, which were conducted in years 2012-2015 (survey A (Lisiak-Felicka, Szmit, 2016)) and 2019 (survey B (Lisiak-Felicka, Szmit, 2021b, pp. 101-115)).

Information security incidents occurred in 18% of offices participating in the survey A and in 25% of offices participating in the survey conducted in 2019 (B). In survey C this percentage has increased to 33%. Increasing number of affected offices may indicate both an increase in the actual number of attacks and an increase in their detection. Considering the large number of attacks reported by CERT and CSIRT teams (compared to the number of incidents in local government offices), it can be expected that the second factor is of great importance here. In previous research offices declared that they reported incidents to computer security incident response teams (CSIRT.GOV.PL and CERT.PL), to police, prosecutor’s office, and Personal Data Protection Office, so the target entities to which the incidents were reported are similar. In survey A there were incidental cases with help from other state administration bodies in the field of incident management. Currently, 16.5% of offices could count on such assistance.

As in the previous studies, officials determined that people (employees) are the weakest link in the security system. The next items are personal data and online services. Analysing the categories of incidents, in both the 2019 and 2023 surveys, the dominant type was malware, followed by intrusions and information content security. The number of offices where cybersecurity training was conducted decreased by 9 percentage points compared to the 2012-2015 (A).

Compared to the previous studies, officials are more optimistic in assessing the level of information security. While previously in 2012-2015 approximately 57% rated it 4 or 5, and in 2019 the percentage of offices that rated this level 4 or 5 was 59%. In the current survey 76% offices rated it as level 4 or level 5 (good or very good).

Financial aspects were also compared. Based on the results, it can now be concluded that the number of offices that allocate marginal funds of PLN 10,000 to financing information security has increased. In 2019 (B) it was 54% of offices, in the current study (C) about 61%.

As in the previous study, the biggest problem in ensuring the appropriate level of security is insufficient financial resources.

6. Conclusions

In conclusion, information security incident management is one of the elements necessary for the proper operation of Information Security Management Systems. To properly manage an incident, it is, of course, necessary to both detect a security breach (the earlier, the better) and respond appropriately, both on the part of appropriate specialists (Digital Evidence First Responders) and employees of the organization that fell victim to the incident. Appropriate response to information security events is one of the issues covered by information security awareness.

Properly responding to incidents requires appropriate preparation before they occur, hence it is necessary to apply a proactive approach that also takes into account potentially new threats in the risk analysis (such as the use of artificial intelligence in conducted attacks, activities related to hybrid warfare, etc.).

The results of research on the elements of ISMS in local government offices in Poland highlight several issues that may lead to security problems and, as it seems, should be of interest to the relevant state authorities.

First and foremost, the insufficient financial resources allocated to cybersecurity are striking. An annual security budget of less than 10,000 PLN is not just extremely low but outright unreasonable (it is lower than the monthly salary of a junior cybersecurity specialist in any commercial company).

Another concerning aspect is the persistently low number of reported information security incidents in offices. When compared to the total number of incidents in Poland and considering the size of local government administration, it can be highly likely assumed that this results not from a high level of security but rather from low detection rates or a lack of reporting of incidents whose consequences can be concealed or mitigated.

Given the above, one may fear that the relatively high self-assessment of the security level might be overestimated.

As part of further research work, it is planned to conduct similar research in other EU countries to compare data on information security management.

Acknowledgements

The results of this study were presented at 15th Scientific Conference. MASEP 2024 (Measurement and Assessment of Social and Economic Phenomena, 27-28.11.2024, Lodz).

References

1. Ali, O., Shrestha, A., Chatfield, A., Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *Vol. 37/1*, https://doi.org/10.1016/j.giq.2019.101419.
2. Banasik, M., Bagińska, J. (2019). Krytyczne uwagi dotyczące bezpieczeństwa infrastruktury krytycznej. *Rocznik Bezpieczeństwa Międzynarodowego*, *Vol. 13, No. 2*, https://doi.org/10.34862/rbm.2019.2.5.
3. CERT.PL (2024). *Krajobraz bezpieczeństwa polskiego Internetu w 2023 roku*. Retrieved from: https://cert.pl/, 1.07.2024.
4. Chodakowska, A., Kańduła, S., Przybylska, J. (2022). Jak polskie gminy radzą sobie z cyberbezpieczeństwem. *Kontrola Państwowa*, *Vol. 67/1(402)*, pp. 129-148. https://doi.org/10.53122/ISSN.0452-5027/2022.1.08.
5. CSIRT.GOV.PL (2024). *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*. Retrieved from: https://csirt.gov.pl/, 1.07.2024.
6. Faifr, A., Januška, M. (2021). Factors determining the extent of GDPR implementation within organizations: empirical evidence from Czech Republic. *Journal of Business Economics and Management*, *Vol. 22 Iss. 5*, pp. 1124-1141. https://doi.org/10.3846/jbem.2021.15095.
7. GOV.PL (2021). *Narodowe standardy cyberbezpieczeństwa*. Retrieved from: https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber, 20.12.2024.
8. GOV.PL (2023). *Baza jednostek samorządu terytorialnego*. Retrieved from: https://www.gov.pl/web/mswia/baza-jst, 26.06.2023.
9. Homburg, V., Kokje, J. (2020). Information policy security compliance in Dutch local government. *Proceedings of the 15th International Conference on Cyber Warfare and Security*, ICCWS 2020 (pp. 211-218). https://doi.org/10.34190/ICCWS.20.025.
10. Hossain, S.T., Yigitcanlar, T., Nguyen, K., Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. *Urban Governance*, https://doi.org/10.1016/j.ugj.2024.12.010.
11. ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary.

12. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements.
13. Jatkiewicz, P. (2015). *Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego*. Warszawa: Polskie Towarzystwo Informatyczne.
14. Klimczuk, O. (2024a). *Atak ransomware na Urząd Gminy w Sokołowie Podlaskim. Danych nie wykradziono?* Retrivied from: https://cyberdefence24.pl/cyberbezpieczenstwo/atak-ransomware-na-urzad-gminy-w-sokolowie-podlaskim-danych-nie-wykradziono, 20.12.2024.
15. Klimczuk, O. (2024b). *Atak hakerski w Jędrzejowie. Starostwo tłumaczy incydent.* Retrivied from: https://cyberdefence24.pl/cyberbezpieczenstwo/atak-hakerski-w-jedrzejowie-starostwo-tlumaczy-incydent, 20.12.2024.
16. Lisiak-Felicka D., Szmit, M. (2021a). GDPR implementation in public administration in Poland – 1.5 year after: An empirical analysis. *Journal of Economics and Management*, *Vol. 43*, pp. 1-21. https://doi.org/10.22367/jem.2021.43.01.
17. Lisiak-Felicka, D. (2024). A Comparative Analysis of Information Security Incidents in Public Administration in Selected European Union Countries. *Management and Administration Journal*, *61(134)*. https://doi.org/10.34739/zn.2023.61.03.
18. Lisiak-Felicka, D., Szmit, M. (2016). *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*. Kraków: European Association for Security.
19. Lisiak-Felicka, D., Szmit, M. (2021b). Zarządzanie bezpieczeństwem informacji w urzędach administracji samorządowej. Główne problemy. In: J. Grubicka, A. Kamińska-Nawrot (Eds.), *Współczesny człowiek wobec wyzwań: szans i zagrożeń w cyberprzestrzeni* (pp. 101-115). Słupsk: Akademia Pomorska w Słupsku.
20. Lisiak-Felicka, D., Szmit, M. (2023). Systemy zarządzania bezpieczeństwem informacji w administracji samorządowej w Polsce – badanie empiryczne. *Przegląd Organizacji, 4,* pp. 390-397. https://doi.org/10.33141/po.2023.04.40.
21. Lisiak-Felicka, D., Szmit, M., Vaińćiuniene, J. (2022). The General Data Protection Regulation 3 Years After Implementation: A Comparison between Local Government Administration in Poland and the Republic of Lithuania. *European Research Studies Journal*, *Vol. XXV, No. 1*, pp. 382-394. https://doi.org/10.35808/ersj/2859.
22. Makowiec, P. (2024). *Świebodzińskie starostwo o ataku: „Ochrona danych jest naszym priorytetem”*. Retrivied from: https://cyberdefence24.pl/cyberbezpieczenstwo/swiebodzinskie-starostwo-o-ataku-ochrona-danych-jest-naszym-priorytetem, 20.12.2024.
23. Marcut, M. (2018). Analysis of GDPR Implementation at County Level. In: C. Harula, C.M. Hinlea, O. Moldovan (Eds.), *Sustainable Development and Resilience of Local Communities and Public Sector Organizations Conference Proceedings “Transylvanian International Conference in Public Administration”*, 16-18 November 2018. Cluj-Napoca, Romania.

24. Martins, F., Amaral, L., Ribeiro, P. (2020). Implementation of GDPR: Learning with a Local Administration Case Study. In: H. Santos, G. Pereira, M. Budde, S. Lopes, P. Nikolic (Eds.), *Science and Technologies for Smart Cities. SmartCity 360 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, *Vol. 323* (pp. 205-216). Cham: Springer, http://doi.org/10.1007/978-3-030-51005-3_19.
25. Microsoft (2023). *Microsoft Threat Intelligence, A year of Russian hybrid warfare in Ukraine.* Retrieved from: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW10mGC, 12.12.2023.
26. NIK (2018). *Informacja o wynikach kontroli Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego.* Retrieved from: https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/pobierz,kap~p_18_006_20180726124543153260914 3~02,typ,kk.pdf, 12.12.2023.
27. Oliveira, M., Dias, G.P. (2023). The role of the data protection officer in local governments: an exploratory study. *18th Iberian Conference on Information Systems and Technologies (CISTI)*. Aveiro, Portugal, pp. 1-6. https://doi.org/10.23919/CISTI58278.2023.10211727.
28. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych [Regulation of the Council of Ministers of 12 April 2012 on the National Interoperability Framework, minimum requirements for public registers and electronic information exchange, and minimum requirements for ICT systems]. (Dz.U. 2016, item.113), Poland.
29. Starčevič, K., Crnkovič, B., Glavaš, J. (2018). Implementation of the General Data Protection Regulation in companies in the Republic of Croatia. *Ekonomski Vjesnik/Econviews*, *Vol. 31(1)*, pp. 163-176.
30. Vestad, A., Yang, B. (2023). Municipal Cybersecurity—A Neglected Research Area? A Survey of Current Research. *Springer Proceedings in Complexity*, pp. 151-165. https://doi.org/10.1007/978-981-19-6414-5_9.
31. Wenlong, Li, Zihao, Li, Wenkai, Li, Yueming, Zhang Aolan, Li (2023). *Mapping the Empirical Evidence of the GDPR's (In-)Effectiveness: A Systematic Review.* Cornell University. https://dx.doi.org/10.2139/ssrn.4615186.