SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2023
ORGANIZATION AND MANAGEMENT SERIES NO. 184

THREATS OF USING INFORMATION TECHNOLOGY IN THE CONTEXT OF PERSONAL DATA SECURITY

Aneta WYSOKIŃSKA[1*], Katarzyna ZAWIERUCHA-KOZŁOWSKA[2]

[1] Faculty of Command Management, War Studies University, Warsaw;
a.wysokinska-senkus@akademia.mil.pl, ORCID: 0000-0001-9021-6355
[2] Faculty of Command Management, War Studies University, Warsaw; k.zawierucha@akademia.mil.pl,
ORCID: 0000-0002-9439-5589
* Correspondence author

Purpose: The article presents security aspects and its essence in the context of personal data protection. Additionally, attention was paid to the use of new technologies and factors generating threats to the use of the mentioned technology in local government units were identified.
Design/methodology/approach: The analysis carried out includes fragments of the doctoral thesis and the results of research carried out within the research topic "Determinants of improving the organization's strategy in the aspect of business continuity management" research task no. II.2.5, War Studies University. The analysis allowed to verify the factors affecting personal data and to identify the causes of potential threats to this data.
Findings: The article identifies factors affecting security and assesses the degree of risk of factors (risk categories) in the context of personal data in the indicated research group.
Practical implications: The research indicates fundamental aspects regarding the essence and importance of security and the importance of topics related to the protection of personal data. Additionally, the presented results classify risk categories according to their importance for personal data.
Originality/value: The information contained in the article discusses the importance of personal data in the world dominated by technology.

Keywords: security, information technology, personal data protection, human resources, information security management system.

Category of the paper: research and review publication.

1. Introduction

Proper protection of personal data plays a key role in the security of IT systems in relations to the functioning of local government units due to the large amount of data processed in their structures using information technology.

http://dx.doi.org/10.29119/1641-3466.2023.184.39

Due to the obligation to secure information resources, local government units are obliged to take a number of actions regarding the processed data. These activities should include activities of a human, organizational, technical and technological nature, as well as those resulting from sudden and unexpected events. When performing public tasks, local government units must also ensure public security, i.e. *a state within the country based on legal norms, in which conditions are ensured for the efficient functioning of a state organization pursuing common, supra-individual goals, obligations are effectively enforced and the rights of individuals living in this organization are protected…* (Fehler, 2010, p. 31).

2. Security, essence and importance

The term security, used to define a state of peace, a state of certainty, i.e. the absence of threats, expresses a subjective nature. However, it is one of the most basic human needs, the satisfaction of which activates higher-level needs. In his theory of motivation, A. Maslow distinguishes safety as the second human need in the hierarchy.

In the most general sense, security is a state in which there are no threats (Żurkowska, 2006, p. 21). M. Lasoń adds that it is a state of peace, certainty of protection against dangers and the ability to defend against them (Lasoń, 2010, p. 9). Nowadays, security is supposed to satisfy human happiness in a holistic sense. It is the paramount necessity and need of all people (Tulibacki, 1999, p. 33). There is no doubt that it is considered one of the basic needs of humans, as well as social groups, the nation and the state (Czuryk et al., 2016, p. 17).

J. Kaczmarek and A. Skowroński drew attention to the etymology of the word security, which comes from the Latin *securitas*. This word, consisting of two elements “sine” meaning “without” and “cura” meaning “care”, defines a state characterized by the absence of worries and the unpleasant feeling of fear (Kaczmarek et al., 1998, p. 17).

The semantic evolution of the word security meant that initially the word meant without concern, without care. Then this meaning changed, shaping its meaning into the statement of being self-confident and brave. Which, in consequence, led to a change in the meaning of the word, from the meaning of without care, without upkeep to not threatened and not threatening. In the Polish language, this was caused by the semantic expansion of the antonym of the word “pieczy” (care) as “niebezpieczny” (dangerous). In the first half of the 14th century, the word opposite to without concern was used with the negation of not or being without concern for existence, for being, i.e. being anxious, feeling insecure. Consequently, the antonym of danger meant free from danger. Therefore, until the end of the 19th century, the word safe meant unthreatened, unthreatening, brave, self-confident (Dominiak, 2007, pp. 192-196).

The multi-aspect nature of security means that this word is defined in various ways, both in Polish and foreign literature. L.F. Korzeniowski defines security as “the objective state of an entity, consisting in the absence of threats, where this state is felt subjectively by individuals and groups” (Korzeniowski, 2012, p. 76). According to P. Gasparski, “security and survival are the most important, cardinal principles of life. Without taking care of security, neither the individual nor the community could exist”, lead a life limited to meeting basic needs. The author suggests that avoiding threats is a basic survival mechanism, treating safety as one of the basic human values, where neglect of safety may suggest a kind of departure from the norm” (Gasparski, 2003, pp. 159-160).

P.D. Williams, in a textbook on security, expresses the opinion that this word is multi-aspected, both ontologically, epistemologically and methodologically. Therefore, security can be treated as a state of control over everything that poses a threat to the values valued by people. This especially applies to threats that, if unattended, could affect the survival of individual entities (Williams, 2008, p. 5).

According to R. Zięba, when deciding about an individual as an inherent subject of the collective, and at the same time the subject and dispenser of the security credo, it can be concluded that *security is the certainty of existence and survival, functioning, development and possession of the entity. The certainty of existence results both from the lack of threats and as a result of the entity’s daily activities; it has the nature of a social process, i.e. it changes over time* (Zięba, 2008, p. 16). The author of this definition combines both the aspects of the state and the process, treating security as the activity of an entity in which the state and sense of security are the result.

J. Świniarski also started to create a definition of security, concluding that *any form of a chosen state of affairs is safe when there is a chance for development and improvement in the perspective of its extension. This perspective depends on both threats and favourable circumstances to counteract, avoid, eliminate, remove or overcome these threats* (Świniarski, 1997, p. 174). The author also notes that this does not only concern threats or their lack, but also on approach that creates opportunities and leads to a longer feeling of security.

Security as a social fact (Moczuk, 2009, p. 70) is defined by E. Moczuk. According to the author, this concept indicates a social system of behaviour of individuals that allows the survival of a specific individual and the entire community, depriving them of the possibility of fear of loss of life, health, statehood, nationality, property, religion, value system and other elements related to a comprehensive understanding of safety, as well as anxiety that these fears will cause fears in others (Moczuk, 2009, p. 70). The mentioned social system of behaviour indicates both the vision of one’s own person, i.e. the individual’s identity, as well as living conditions ensuring a high standard of life and a sense of satisfaction in the cultural sphere.

3. Information security in the context of personal data protection

Information security is often perceived as part of the IT system. Calling it network security, computer security, telecommunications security, data security, etc. (Janczak, Nowak, 2013, p. 17).

Information security includes elements of information security and ICT security, i.e. IT security (systems) and ICT network security. Information security is the protection of all forms of data exchange, storage and processing. ICT security is limited to technical ICT means, ICT systems, computer systems (IT security) and ICT networks (ICT network security) used to exchange, store and process data in electronic form (Janczak, Nowak, 2013, p. 17).

IT security is therefore the security of communications, and IT security defines the security rules defined for the software and hardware of a computer system to protect against manipulation, disclosure, deletion, data modification or denial of service (Janczak, Nowak, 2013, p. 45).

According to the Personal Data Protection Office and the PN-ISO/IEC 27000 standard, personal data security is information security supervision, i.e. a system through which the functioning of an organization (its activities) in the field of information security is controlled and directed.

The enormous progress of civilization, which has brought transformations in the management of organizations, has caused these organizations to transform, make changes and adapt to new standards. This applies to both the civil economy as well as organizations and institutions operating in the area of security management. Undoubtedly, the most important factor causing changes is the technological factor. Technology means a field of technology that deals with the design and modelling of new production methods or methods of processing raw materials. Thus, new technologies mean the use of the latest results resulting from knowledge of science in connection with conducted research and their application in practice.

It is worth noting that currently virtually all organizations undertake activities aimed at supporting management processes. These processes mainly concern the improvement and streamlining of management in the area of logistics, finance and human resources, where the use of modern IT solutions facilitates rational management (Kuck, 2012, p. 186).

The use of modern technologies in management is applicable both from a strategic and operational perspective. The essence and role of technology is of great importance in modern and innovative management, where knowledge of the potential of technology and its impact on creating competitive advantages, building business models as a tool for competing in an enterprise enables management in diverse economic conditions.

Organizations that support technology and digitalization result in positive economic growth, meet the expectations of contractors and achieve higher profits. However, those using old management models are often doomed to failure. The development of technology very often precedes other economic sectors and concepts in the field of social sciences, yet politics and law should support the development of technology. Therefore, it is worth investing in technologies, digital business and an environment that will constantly develop in this aspect.

New technologies used in the economic market are very often combined with information technology (IT), which allows the processing of information between devices and users of these devices. Additionally, it stores and secures the acquired information for later analysis and presentation, so that the right information can be delivered to all interested parties. Fast and reliable access to information is a huge advantage of enterprises that process data at the right time, at the right decision-making level and at the same time ensuring the required level of security. In this aspect, it seems necessary to use modern information technologies that enable the exchange of all types of data through computer networks of specific organizations.

Modern technologies support management processes, enable efficient management of projects implemented in organizations, provide necessary information, secure the organization’s financial resources and provide the opportunity to exchange experiences. Additionally, they facilitate the implementation of purchases made by the organization, provide the opportunity to prepare and conduct training for employees on, for example, personal data protection, which are aimed at improving the security of processed information and facilitate human resources management. New technologies are also the Internet of Things, very often used in the main sectors of the national economy: trade, transport, industry, science, education, health care, administration and agriculture, providing the opportunity to integrate the systems of manufacturers and recipients.

New technologies in organization management allow for the identification of ongoing projects, determining the necessary resources indicating the correctness of performing a specific task, and provide the opportunity to search for optimal ways of implementing activities. They create a system for managing the security of processed information, ensuring information security and ICT security, while ensuring continuous availability, confidentiality, integrity and resilience of services and systems used for data processing.

The basis for proper management of an organization in the era of modern technologies is the appropriate use of IT systems, which become their integral part. The construction of an appropriate management system should be based on the development and implementation of an informatization strategy, i.e. the appropriate relationship between people, resources (including technological ones) and management methods enabling the achievement of intended goals within a specified period of time. This concerns the following elements (Kuck, 2012, p. 188):

- the current state of computerization for the organization,
- direction of development of computerization,
- basics of an IT system to support specific processes,
- the effects of computerization and the strategic goals of the organization.

Modern technologies in organizational management should only be limited to improving the quality of enterprise functioning and having a positive impact on the information security management system (ISMS), which is the basis for the functioning of organizations dominated by modern technologies. This system integrates with other systems supporting the functioning of the ISMS (Wołowski, Zawiła, Niedźwiecka, 2012, p. 17). In a world dominated by technology and big data analytics, the importance of an information security management system stems from the validity of personal data protection regulations of all organizations processing data (both customers and employees).

4. Research methodology

The aim of the study is to identify threats that may occur when using information technologies in the context of personal data protection; determining which of these threats pose the greatest threat to personal data processed in the analysed organizations and identifying technological factors that influence the increase in the level of security in the context of personal data protection.

The research used a diagnostic survey method using a questionnaire, which was addressed to personal data protection inspectors and personal data administrators as well as people with knowledge in the field of personal data protection in all Polish local government units processing personal data.

The target population of local government units included 2807 entities, consisting of municipal governments (2477), district governments (314)[1] and voivodeship governments (16). The minimum sample size with a known population size – 2,807, maximum allowable estimation error – 5% and confidence coefficient – 95% was estimated at 338 units according to the formula:

$$n_{min} = \frac{p(1-p)}{\frac{d^2}{z^2_{1-\frac{\alpha}{2}}} + \frac{p(1-p)}{N}},$$

where:

$p -$ estimated fraction size,

$d -$maximum allowable estimation error,

$N -$ size of the general population,

$z_{1-\frac{\alpha}{2}}$ – quantile of the $1-\frac{\alpha}{2}$ order in a standardized normal distribution $N(0{,}1)$.

[1] Cities with country rights are included in the municipal government.

Ultimately, in the study carried out for the purposes of the doctoral dissertation, the survey was sent to 372 local government units representing municipal, district and provincial governments in all voivodeships. It was taken into account that in order to maintain representativeness, the structure of the research sample according to the voivodeship and the type of local government unit should largely correspond to the structure of the entire population.

The study involved 177 women, representing 47.6% of respondents, and 195 men, representing 52.4% of respondents.

The majority of respondents were people between 41-50 years old (35.5% of respondents) and 31-40 years old (32.5% of respondents). The youngest group consisted of respondents under 20 years of age (0.03% of respondents), which is also the smallest group. The oldest group were people over 50 years old (23.1% of respondents), and the group was between 20-30 years old (8.6%).

Most respondents responded from local government units operating in rural areas, which constituted 170 local government units (45.7%). A city under 20,000 inhabitants (small town) was represented by 108 local government units (29%), a city of 20-99.9 thousand inhabitants (medium-sized city) was represented by 72 local government units (19.4%), a city with over 200,000 inhabitants (large city) by 12 local government units (3.2%). The smallest group were representatives from the city of 100-199.9 thousand inhabitants (large city) by 10 local government units (2.7%).

4.1. Research Findings

The conducted research allowed for the identification of factors that generate threats in the context of personal data protection in local government units.

As can be seen in Fig. 1, according to the surveyed local government units, the human factor resulting from the possibility of accidental, unintentional disclosure of personal data is a key risk category that may have a negative impact on the personal data protection process. Analysis of this chart shows that 63% of entities considered this factor to be at least a major threat to the functioning of local government units, with the majority of them defining this risk category as a very major threat. Only 1% of individuals considered that the human factor does not constitute any threat from the point of view of personal data protection, and 18% consider it to be at most a small threat.

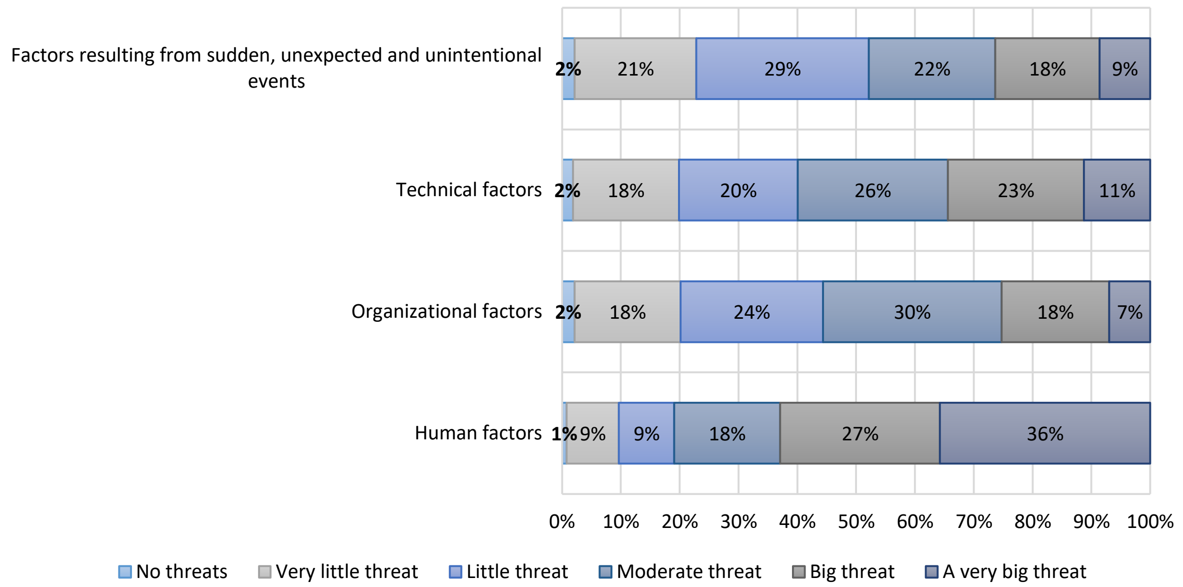

Figure 1. Distribution of answers to the question what factors (risk categories) pose the most threats in the context of personal data protection in local government units.

Source: own study based on conducted research.

In the context of other risk categories that may have a negative impact on the personal data protection process, it can be noted that they generally pose a moderate threat at most. This applies to both organizational factors (resulting from the adopted organizational structure, applied technical and technological solutions), technical factors (resulting from the adopted methods of securing rooms, operating devices, the method of organizing exits and entries to rooms and buildings, closing cabinets, rooms and other places) as well as those resulting from sudden, unexpected or unintentional events.

34% of local government units consider technical factors to be at least a major threat. In the case of factors resulting from sudden, unexpected and involuntary events and organizational factors, only 27% and 25% of individuals respectively consider them a risk category of at least a high risk in the context of personal data protection. With regard to factors resulting from sudden, unexpected and no-fault events, technical and organizational factors, local government units usually considered them to be risk categories carrying low risk (no threat, very low risk and low risk). Respectively, 52%, 40% and 44% of the surveyed units indicated this level of threat.

The above observations are confirmed by the assessment of the degree of risk of factors (risk categories) in the contest of personal data protection in local government units, expressed as an arithmetic mean[2].

[2] The following coding method was adopted: 0 – no threat, 1 – very little threat, 2 – little threat, 3 – moderate threat, 4 – high threat and 5 – very high threat.

Of all four key factors that pose a threat to local government units from the point of view of personal data protection, the human factor turned out to be the most important. This is evidenced by the high value of the average, which is a measure of the assessment of the degree of threat, which was 3.7 for this risk category. It is worth mentioning that for the human factor, the dominant response was 5 and the median was 4. This means that local government units most often considered the human factor to be a very high risk in the context of personal data protection, and 50% of them considered it to be at least a major threat. For the remaining risk categories considered (factors resulting from sudden, unexpected, no-fault events, organizational and technical factors), the risk level expressed as an average was at the level of 2.6-2.8.

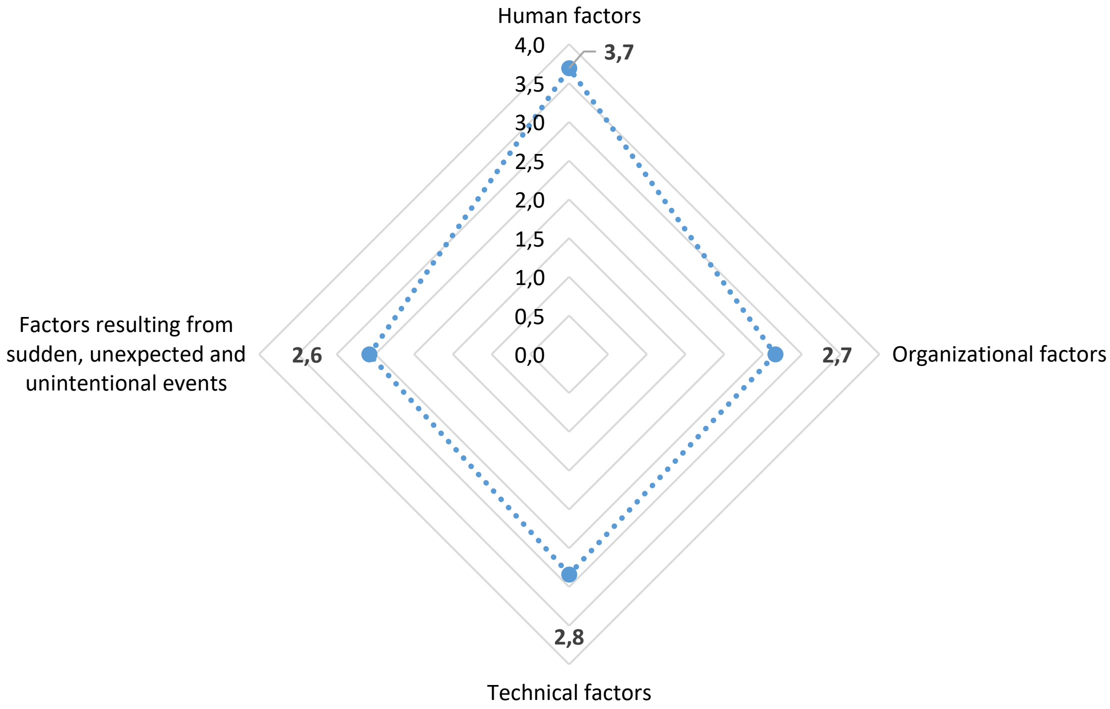

Figure 2. Assessment of the degree of risk of factors (risk categories) in the context of personal data protection in local government units.

Source: own study based on conducted research.

It is worth emphasizing that for organizational and technical factors, the dominant was 3 (moderate threat), as was the median – 3. In the context of factors resulting from sudden, unexpected and involuntary events, the dominant and the median were even smaller and amounted to 2 (low threat).

The conducted research made it possible to isolate the most important technological factors (information technologies) influencing the improvement of the systemic approach and increasing the level of security in the context of data protection in local government units. For the purposes of the study, exploratory factor analysis was used once again.

The factor extraction process began with assessing the significance of the correlation matrix. For this purpose, the Barlett's test of sphericity was used, which is one of the tools used to assess the validity of using factor analysis. The p-value determined in Barlett's test of sphericity was 0.000[3] and is lower than the significance level adopted for the analysis $\alpha = 0{,}05$. The null hypothesis that all correlation coefficients are equal to zero should therefore be rejected. The adequacy of the correlation matrix was then assessed using the Kaiser-Mayer-Olkin (KMO) coefficient. The degree of adequacy measured by the KMO coefficient was 0.94. We therefore have a strong basis for using factor analysis. Further in the study, the main factors of information technology that influence the improvement of the systemic approach and increase the level of security in the context of data protection in local government units were identified. For this purpose, the principal components method with Varimax factor rotation was used to determine the factors.

First, the number of factors was determined. For this purpose, the halfway criterion and the scree criterion were used, according to which we are looking for a place from which there will be a gentle decline in eigenvalues to the right, i.e. a place from which the so-called "factorial scree" is located to the right. By analysing figure 3 it can be seen that the "scree" phenomenon most likely occurs with the second or third factor. To the right of this place there is a slight decline in eigenvalues.

In the process of isolating the main information technology factors that influence the improvement of the systemic approach and increase the level of security in the context of data protection in local government units, it was finally decided to select three main factors that allow to explain approximately 73% of the total variability (Table 1). According to the so-called half criterion it is also a sufficient number of factors that can be subject to substantive assessment[4].

[3] For the purposes of the analysis, it was rounded to three decimal places.

[4] According to the half criterion, it is enough to isolate enough factors to explain at least 50% of the total variability. Therefore, the analysis could include two factors based only on this criterion. However, based on the scree and half criteria, it was considered more rational to take into account three factors that explain much more variability than two factors.

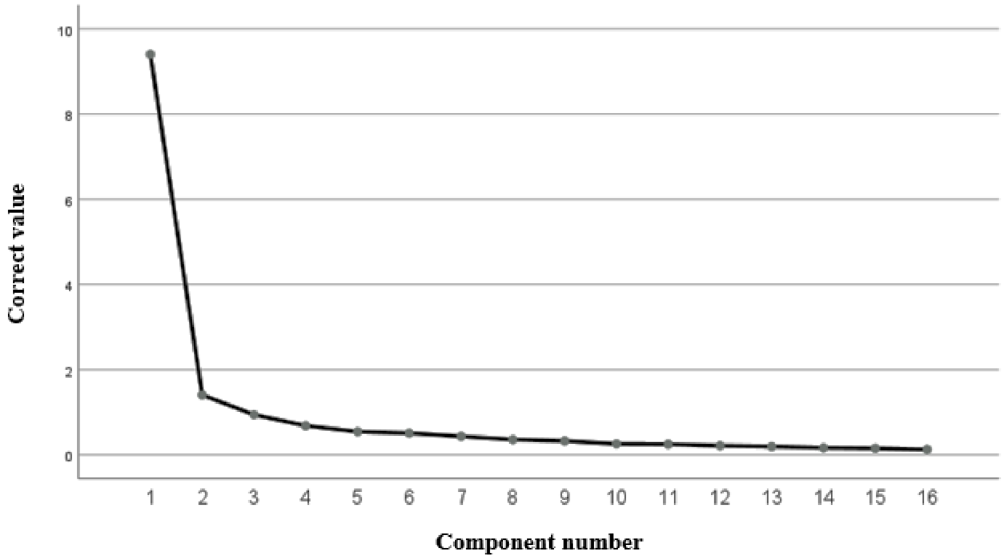

Figure 3. The scree plot in the analysis of the most important technological factors influencing the improvement of the systemic approach and increasing the level of security in the context of data protection in local government units.

Source: own study based on conducted research.

Table 1.
Total explained variance in the analysis of the most important technological factors (information technologies) influencing the improvement of the systemic approach and increasing the level of security in the context of data protection in local government units

Component	Total	% variance	% cumulative
1	4.549	28.430	28.430
2	4.493	28.079	56.509
3	2.717	16.982	73.491

Source: own study based on conducted research.

The factor corresponding to the first (largest) eigenvalue explains approximately 28.4% of the total variance, the second component explains approximately 28.1% of the total variance and the last third component explains approximately 17% of the total variance. Taking into account the scree and half criteria, three factors were finally identified, which explain a total of 73% of the total variance.

When summarizing the analysis performed, it can be noted that there are three key factors (groups) of information technologies that influence the improvement of the systemic approach and increase the level of security in the context of data protection in local government units (Figure 4).

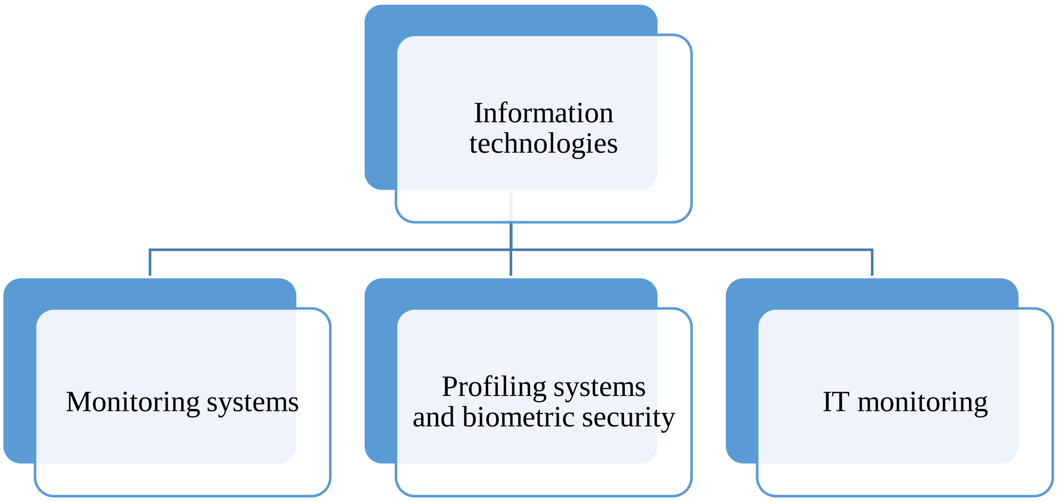

Figure 4. Information technologies influencing the improvement of the systemic approach and increasing the level of security in the context of data protection in local government units.

Source: own study based on conducted research.

Therefore, local government units recognize the need to use modern solutions in the field of information technology to maximize the degree of protection of individual data, while minimizing the risk of their disclosure to third parties. However, they are aware that their development, especially in relation to IT monitoring and biometric security, may also constitute a source of threat to the security of personal data. This may be due to the fact that, on the one hand, local government units see great potential and the need to improve technological solutions in the context of personal data protection, and at the same time they notice certain threats that this development creates (the development of technology generates gaps in the data protection system, the applicable regulations are not adequate to the current state of new technologies).

4.2. Discussion

Summarizing the analysis carried out, it can be clearly stated that the factor limiting the effectiveness of personal data protection using information technology is humans. Local government units consider the human factor to be crucial and likely to pose the greatest threat in the context of personal data protection.

In the literature, the most common causes of potential threats are mentioned (Bógdał-Brzezińska, 2012, p. 7):

- improper protection of services, cryptographic devices and auxiliary devices,
- damage to devices and/or telecommunications lines,
- inappropriate or insufficient software,
- gaps and errors causing data loss,
- lack of user awareness of IT security, validity of processed data, possibilities of personal data protection, expected penalties related to violations, etc.,
- intentional damage to IT systems,
- intentional attacks,

- short technology life,
- conscious incidents committed by users (managerial staff, employees), e.g. connecting devices to an unsecured network or connecting external devices containing malicious software,
- unauthorized actions of administrators and/or users.

M. Soczko takes into account the following threats based on the frequency of incidents (Soczko, 110):

- disclosing personal data to unauthorized persons,
- inability to access personal data by authorized persons,
- destruction, damage or alteration of personal data,
- operation of malicious software (keyloggers, viruses, Trojans, etc.),
- intrusion of an unauthorized person into the data processing area,
- social engineering attacks,
- attempts to extort data and/or data security methods,
- loss, damage or theft of media, backup copies and devices containing data.

As K. D. Mitnick and W.L. Simon note in their book, despite purchasing the most expensive and best security technologies, using services that protect the organization, the training employees in terms of confidentiality of the acquired data, the organization still remains unsecured. Similarly with private persons. They can implement all kinds of rules that are recommended by experts, configure the system, install security programs, use all kinds of permissions and also remain unsecured. The authors note that the Achilles heel of security systems is the human factor. Security, through people's naivety, ignorance, recklessness, or gullibility, often becomes an illusion (Mitnick, Simon, 2003, p. 24).

5. Summary

Changes taking place in the modern world have made information technology play a huge role in human functioning, and personal data have become a kind of modern currency. It is very easy to lose or leak personal data, it is an irreversible process, which is why it is so important to comply with the provisions on the protection of personal data and to promote the code of good practices in the use of information technologies in the context of personal data protection.

Personal data protection regulations in local government units are often unknown or known only to a small or moderate extent. However, it is worth realizing that the processing of data by persons who do not have appropriate knowledge in the field of personal data protection does not guarantee their protection and security of processing.

In order to improve the quality of the management process and minimize the risk of threats to personal data security resulting from the use of information technologies, a comprehensive approach is proposed by implementing and certifying an information security management system.

Statistics show that despite the growing number of certificates granted for compliance with the ISO 27001 standard worldwide, the share of certificates granted in the Public administration sector is relatively small compared to other sectors.

Therefore, it is recommended to pay attention to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the Information Security Management System, because a properly implemented and certified system brings many benefits to the organization that contribute to improving the quality of management and increasing the organization's security level.

References

1. Bógdał-Brzezińska, A. (2012). *ICT threats to Poland's security. Internal and international conditions,* https://www.researchgate.net/publication/333581869_Teleinformatyczne_zagrozenia_bezpieczenstwa_Polski, 5.09.2023.
2. Czuryk, M., Dunaj, K., Karpiuk, M., Prokop, K. (2016). *State security. Legal and administrative issues.* Olsztyn: Faculty of Law and Administration, UWM.
3. Dominiak, G.A. (2007). The appearance of ontological security – glosses. In: A. Dobosz, A.P. Kowalski. *Ontological security*. Bydgoszcz: Epigram.
4. Fehler, W. (2010). *Public security as a component of internal state security. Security. Theory and Practice.* Kraków: Printing House.
5. Gasparski, P. (2003). *Psychological determinants of readiness to prevent threats*. Warszawa: PAN.
6. Janczak, J., Nowak, A. (2013). *Information security. Selected problems.* Warszawa: National Defense Academy.
7. Kaczmarek, J., Skowroński, A. (1998). *Security: World-Europe-Poland*. Wrocław: Atla 2.
8. Korzeniowski, L.F. (2012). *Basics of security sciences*. Warszawa: Difin.
9. Kuck, J. (2012). Modern technologies and innovation in management processes. In: T. Jalowiec, W. Nyszk. (eds.), *Innovations in the management of logistics processes of the armed forces.* Warszawa: AON.
10. Lasoń, M. (2010). Security in international relations. In: E. Cziomer, *International security in the 21st century. Selected problems.* Kraków: AFM Publishing house.
11. Mitnick, K.D., Simon, W.L. (2003). *The art of deception.* Gliwice: Helion.
12. Moczuk, E. (2009). *Sociological aspects of local security.* Rzeszów: Urz.

13. Soczko, M. (2017). Personal data protection as an element of information security. In: *Vademecum ABI Part II – Preparation for the role of the Data Protection Inspector*. Warszawa: C.H. Beck.
14. Świniarski, J. (1997). *On the nature of security. Prolegomena to general issues*. Warszawa: Ulmak.
15. Tulibacki, T. (1999). Ethical aspects of security against the background of certain “permanent” features of human nature. In: R. Rosa, *Education for security and peace in a uniting Europe. Theory of its application.* Siedlce: Institute of Pedagogy of the Higher School of Agriculture and Pedagogy in Siedlce.
16. Williams, P.D. (2008). Security research. Introduction. In: P.D. Williams, *Security studies*. Kraków: UJ.
17. Wołowski, F., Zawiła-Niedźwiecki, J (2012). *Security of information systems. A practical guide in accordance with Polish and international standards*. Kraków/Warszawa: edu-Libri.
18. Zięba, R. (2008). *International security after the Cold War*. Warszawa: WaiP.
19. Żurkowska, K. (2006). The concept of security and its evolution. In: K. Żurkowska, M. Grącicki, *International security theory and practice*. Warszawa: Warsaw School of Economics.