SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 224

ARTIFICIAL INTELLIGENCE IN SMALL ENTERPRISE MANAGEMENT – CYBERSECURITY CHALLENGES

Elena MIESZAJKINA[1*], Małgorzata PIKUL[2], Karolina OSTAPIŃSKA[3], Bohdan KULCHYTSKYY-DASHYNYCH[4]

[1] Lublin University of Technology; e.mieszajkina@pollub.pl, ORCID: 0000-0002-3449-4059
[2] Lublin University of Technology; m.pikul@pollub.pl, ORCID: 0009-0004-1595-8876
[3] Lublin University of Technology; k.ostapinska@pollub.pl, ORCID: 0009-0006-5959-8467
[4] Lublin University of Technology; s96777@pollub.edu.pl
* Correspondence author

Purpose: Enterprises' use of digital technologies requires cybersecurity measures to protect data, systems, and users from cyber threats. The article aims to present theoretical considerations and empirical research results on cybersecurity management in small enterprises using digital tools in their operations.
Design/methodology/approach: The research was based on two methods. The analysis and literature criticism method allowed for exploring the topic's theoretical basis and developing the methodological assumptions of the empirical study. It was conducted using a diagnostic survey method with a structured interview technique.
Findings: The research analyzed small business cybersecurity challenges. The main problems were found to be limited budgets and the occurrence of complex and dynamic cyberattacks. It is necessary to improve employees' digital competence and cybersecurity awareness.
Research limitations/implications: The survey was a pilot study. It allowed for the verification of the research assumptions and the research tool. The study revealed the relevance of the discussed topic and the need for further in-depth analysis. It is necessary to clarify the survey tool and repeat the survey on a larger sample.
Practical implications: The article examines the aspects of cybersecurity management in small enterprises. It identifies key issues and demonstrates the need to implement practical solutions to prevent cyberattacks.
Originality/value: The value of the article is the development of a research concept enabling a holistic assessment of practices and challenges in the management of cybersecurity of small enterprises in the context of the use of artificial intelligence.
Keywords: cybersecurity, cyberspace, artificial intelligence, small enterprises.
Category of the paper: Research paper.

1. Introduction

With the rapidly changing business environment, small enterprises are confronted with numerous challenges resulting from global social and economic changes and increasing digitization. Turbulent times require not only the ability to adapt flexibly but also the ability to anticipate and respond quickly to changing market conditions. The modern world is described using the BANI (Brittle, Anxious, Non-linear, Incomprehensible) concept, created by J. Cascio (2022). In these circumstances, traditional business models and business methods may prove to be insufficient. Small enterprises, often struggling with limited resources, need to implement modern technologies to increase their resilience to sudden changes and compete effectively in the marketplace. Artificial intelligence (AI) is a supporting tool for these activities. It facilitates rapid processing and analysis of large datasets, automates decision-making processes, and predicts market trends (Mieszajkina, Ostapińska, 2024).

AI is a widely analyzed issue in scientific, journalistic, and political contexts. It involves knowledge modeling, data processing, and algorithm and computational system development, enabling the automatic acquisition, analysis, and use of information. Modern AI systems are characterized by their ability to self-learn, predict patterns based on collected data, and interact with the external environment through sensors and actuators. This process can be conducted autonomously or with human involvement at various stages of the AI life cycle - from design, implementation, and operation, to shutdown and disposal (Portal Sztucznej inteligencji, 2025a).

Understanding AI's capabilities is no longer exclusively the domain of modern technology specialists. Nowadays, it is one of the most important subjects of public debate, as it significantly influences socio-economic transformation processes (Digital Sustainability Forum, 2019). AI has revolutionized the traditional approach to running a business, contributing to the implementation of innovative solutions in various economic sectors. Enables modern business model creation, supports optimization processes, increases operational efficiency, and builds sustainable competitive advantage. It contributes to maximizing profits and dynamic enterprise development.

The first attempt to define the term “artificial intelligence” was made in 1955 by American computer scientist John McCarthy at the Dartmouth Conference, a research workshop dedicated to developing machines capable of intelligent behavior. He described it as „the science and engineering of making intelligent machines” (IAPP, 2023). Currently, the term, despite its widespread usefulness, remains difficult to define clearly because the concept of “intelligence” itself is not precisely defined.

Throughout the years, numerous AI definitions have appeared, reflecting different research approaches. Early approaches focused on the ability of machines to perform functions traditionally reserved for humans (Rich, Knight, 1990). According to R.J. Schalkoff (1990), AI seeks to explain and emulate intelligent behavior through computational methods. Slightly

later, R. Kurzweil (1999) expanded the definition, listing a wide range of systems in the AI area (systems with knowledge base, expert systems, image recognition, machine learning, language recognition, robotics). However, N.J. Nilsson (2014), one of the leading researchers in the field, emphasizes that AI supports the structuring and design of intelligent machines that imitate human intelligence.

In a practical interpretation of the SAS Analytics Platform (2025), AI is considered a technology that allows machines to learn from experience, adapt their actions to new data, and perform tasks typical of humans, such as inference, discovering hidden relationships in data or solving complex problems. Similarly, the PWN Polish Language Dictionary (2025) defines AI as "a branch of computer science that examines the rules governing human mental behavior and creates programs or computer systems that simulate human thinking".

Currently, there is no uniform AI definition in both national legislation and international regulations. A systems approach dominates the literature. This model has been adopted by the OECD, among others, and is reflected in Poland's AI policy. It is interpreted as a system based on the machine concept, which can influence the environment by making recommendations, forecasts, or decisions regarding set goals. It operates on inputs, both machine and human, to: 1) understand real or virtual environments; 2) transform this information into models (manually or automatically); 3) use these models to formulate various outcome options (Portal sztucznej inteligencji, 2025a).

Summarizing these and other AI definitions, it can be concluded that they have evolved from general concepts of automating human activities and functions to more precise approaches involving specific technologies and methods. Despite the differences, the common thread is the perception of AI as systems capable of imitating human cognitive processes to varying degrees of sophistication. As T. Zalewski (2020) indicates, it is more beneficial to emphasize AI's practical applications in various aspects of our lives rather than focusing on precise definitions.

Are small enterprise executives aware of the challenges of operating in an environment of widespread digitization? Do owners and managers see the potential of AI as a tool to increase innovation and growth opportunities for their businesses? Are they aware of the risks involved and are they taking action related to cybersecurity? To answer these questions, a pilot study was conducted to analyze and assess cybersecurity management practices, challenges, and gaps in small enterprises. The originality of the presented considerations lies in the application of a holistic approach to cybersecurity integrating social, organizational and technical-technological dimensions. The need for continuous development of digital competences of employees of small enterprises was also emphasized.

2. Using AI in small business

AI is playing an increasingly important role in enterprises' operations, radically transforming the way they operate, make decisions, and interact with stakeholders. Its impact on business goals is noticeable in large and small economic organizations. Using advanced machine learning algorithms allows products and services to be adjusted to individual consumer expectations. Personalization increases their satisfaction and engagement, which is especially important in a small business (Krystian, Zaskórski, 2023). E. Bielinska-Dusza (2022) indicates such benefits associated with AI use as process automation and advanced data analysis. Routine task automation allows employees to focus on strategic activities. Processing and analysis of large data sets gives the opportunity to better understand market trends, and customer preferences and optimize marketing activities. Forecasting future trends and changes, predicting sales, and supporting business planning processes are also important AI applications. This allows entrepreneurs to manage resources more efficiently, undertake thoughtful marketing and investment activities, and optimize employment. With AI development, enterprises are gaining access to increasingly sophisticated analytical tools to better understand the mechanisms shaping demand and predict consumer response to the products and services on offer. These include, among others (Wodecki, 2018, 2021):

- product recommendation systems used by online platforms,
- automating customer service with chatbots and virtual assistants,
- monitoring social media for feedback on products and services offered,
- personalization of advertising content and conversion prediction, enabling more effective outreach to precisely defined target groups.

In recent years, there has been a rapid increase in AI tools used in Poland. This is confirmed by the data from the global organization PricewaterhouseCoopers' report “Ready for Artificial Intelligence”. Three-quarters of Polish companies have begun implementing AI technologies, mainly to automate processes, detect anomalies and improve prediction quality. However, it should be noted that most of them are only in the early stages of implementation, and only a few are using AI to its full potential. More than half of enterprises (55%) have defined an AI strategy or are working on developing one. This confirms the growing awareness that digital technology use is key to realizing the intended business and financial benefits (PwC, 2024).

The “Power of AI” report published by BUZZcenter (2024) revealed that 77% of surveyed enterprises experience a positive AI impact on their growth. Publicly available AI tools are used by 43% of respondents, solutions adapted to specific enterprise needs are used by 20%, and 14% have implemented dedicated AI tools. Only 15% of respondents declare not using AI currently, but plan to implement its tools in the short term, while 8% of respondents are not using this type of technology and do not intend to implement it. The report's authors emphasize that companies recognize AI's potential, indicating its benefits such as time savings, process

automation, reduced operating costs, predictive capabilities, innovation, better risk management, and improved product and service quality.

The 2024 "Business Digital Transformation Monitor" research was conducted by a global organization of independent enterprises KPMG in partnership with Microsoft. They were attended by 180 managers who are responsible for digitization issues in their organizations. Large enterprises were represented by 31% of people, medium enterprises by 39%, and small enterprises by 30%. Nearly a third of respondents declared they would use AI tools, while another 30% plan to implement them in the current year. Smaller enterprises tend to implement these technologies at a lower level, not because they are unaware of their importance, but due to limited resources and insufficient experience in digitally transforming their organizational processes. Certainly small business needs more support in achieving digital maturity (KPMG, Microsoft, 2024).

According to a survey conducted by AI Chamber (2024) among 350 decision-making employees of small and medium-sized enterprises (SMEs) from Poland, the Czech Republic, Estonia, and Romania, 9 out of 10 surveyed entities are using AI and machine learning (ML), with one in four using it to a significant degree. This has a positive impact on the following areas of their business: IT, marketing, customer service, administration, sales, logistics, production, quality control. Two-thirds of survey participants are convinced that AI and ML positively impact their businesses. Half of the respondents see the potential of these technologies to build competitive advantage, and more than 40% predict positive financial effects from their implementation. Only 4% of respondents have a negative perception of AI and ML. However, implementing AI tools in SMEs is associated with certain difficulties. These include, for example, lack of confidence in digital technologies, high implementation costs, lack of adequate infrastructure, inadequate staff competence, and difficulty in recruiting qualified professionals.

E. Bielinska-Dusza (2022) also emphasizes that despite the growing use of AI technologies in both large and small enterprises, the process still encounters numerous barriers. She divides them into four types:

1. barriers resulting from the AI technology's limitations (related to the state of the existing knowledge and scientific and technological base),
2. intra-organizational barriers (strategic, resource, and time pressure related to the development and implementation of digital tools),
3. external barriers (from the environment),
4. hybrid barriers, resulting from the interaction of the first three.

L.S. Dalenogare et al. (2018) emphasize that overcoming barriers requires not only identifying them, but first and foremost understanding their causes, effects, and multidirectional interrelationships that hinder AI technology implementation.

The Ministry of Development and Technology, with support from the European Commission under the Technical Support Instrument, has implemented the project "Advancing The Digital Transformation of Polish Enterprises" (2024). The research results confirm that the digitization advancement level of SMEs in Poland is low, with its pace limited by financial, resource, technological, organizational, competence, and psychological factors.

Many digitization barriers result from the specific SME characteristics (Mieszajkina, 2020). Entities in this sector most often finance their operations from their resources and have little access to the capital market, which limits their ability to invest in digitization. Many entities lack sufficient knowledge of available EU funding sources. The decisive owner's role and lack of ability and willingness to delegate authority result in one-man decision-making, with a focus on day-to-day operations instead of strategic development. Lack of process formalization and action planning means that digitization is not a priority, and actions are ad hoc and unsystematic. Several technological barriers are related to inadequate and mismatched infrastructure to the business nature, as well as the lack of professionals with the appropriate digital skills. SMEs typically do not employ staff with specialized IT training, and owners' knowledge of new technologies is often limited. Digital competence development is based on short-term market needs and on taking advantage of emerging training opportunities. This is not conducive to gaining strategic knowledge and skills in AI and cybersecurity. Consequently, many decisions regarding the digitization of operations rely on intuition rather than analysis and strategic planning. Moreover, the small scale of operations and labor-intensive nature of production lead to technologies being treated as an unnecessary cost rather than an investment in development (Mieszajknia, Bochen, 2022; Scoutto et al., 2021). All this makes digital transformation chaotic, without clearly defined goals and plans.

Despite the clear barriers, SMEs have the potential to reap significant benefits from the implementation of digital and AI tools, such as increased productivity, reduced costs, increased customer satisfaction, and enhanced competitiveness. By doing so, they can greatly enhance their chances of achieving success and strategic growth.

3. Artificial intelligence challenges - cybersecurity

Advances in AI bring new opportunities, challenges, and threats to its users. A significant problem is the increasing risk of committing crimes related to security breaches of processed information and the misuse of mass media to disseminate prohibited content. Crimes involving the instrumental use of networks and information systems to violate legally protected interests under criminal law are also a significant threat (Siwicki, 2012). Therefore, it is important to take action to secure the cyberspace in which enterprises operate.

Over the years, numerous theoretical concepts and analytical approaches to cyberspace have developed. M. Jurek (2023) considers it from two perspectives. In a broad (abstract) sense, he defines it as a global information infrastructure that enables people to connect through computers and telecommunications. In a narrower sense - as a communication space created by a system of Internet links, facilitating users to interact in the real world. Similarly, P. Sienkiewicz (2009) considers cyberspace as a kind of communication space created by a system of Internet connections. He indicates two aspects:

1. positive, in which it is an area for cooperation on many levels (including social, economic or security),
2. negative, taking various forms (including cybersurveillance, cybercrime, cyberterrorism or cyberwarfare).

According to the U.S. Department of Defense, cyberspace is a global domain in the information environment, consisting of an interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processes and controllers (Ottis, Lorents, 2010).

C. Banasiński (2018, p. 31) understands the term cybersecurity as "the process of ensuring the safe functioning in cyberspace of the state as a whole, its structures, individuals, legal and other entities, and information resources in global cyberspace". R.A. Kemmerer (2003, p. 3) believes that „cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders". J.A. Lewis (2006, p. 1) defines it as „cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and malicious damage or disruption". E. Amoroso (2006) emphasizes that for ensuring cybersecurity, activities, technologies, and practices are necessary to minimize the risk of malicious attacks on information systems. This includes a variety of protection mechanisms such as intrusion detection and prevention systems, anti-virus software, solutions to block unauthorized access, multi-component authentication mechanisms, and technologies to ensure secure and encrypted communications. According to D. Craigen and N. Diakun-Thibault (2014), understanding the nature of cybersecurity requires a multidisciplinary approach. The phenomenon is adversarial, where some users aim to protect computer systems, while others utilize information technology to breach their security features. Effective protection cannot be limited to traditional disciplines such as mathematics, computer science, or electrical engineering, but requires interdisciplinary analysis.

C. Banasinski and M. Rojszczak (2023) define cybersecurity as a multidimensional process involving integrated measures to protect against threats from cyberspace. The authors emphasize that effective digital security requires technical, legal, and organizational measures to respond to dynamically evolving challenges and threats effectively. Their analysis highlights the complexity of protecting both data and infrastructure and information, indicating the need to improve strategies and tools to effectively counter cyberattacks continuously.

The threat of cyber attacks, data breaches, and digital content theft is a concern for all organizations. In the US, 43% of all cybercrime incidents target SMEs. A major factor undermining security systems is the human element—often it is not the IT systems, but users who represent the weakest link in the cybersecurity framework (PBSG, 2021).

According to the taxonomy proposed by W. Nowak (2020), cybersecurity incidents can be divided into three groups: 1) malware attacks; 2) identity theft; and 3) attacks that block access to services. Their main goals are to steal data, disrupt operations, cause financial damage, and permanently or temporarily disable systems.

Organizations belonging to different sectors and operating in different industries process increasingly large sets of data in the course of their business activities. This trend intensified during the pandemic, when most operations were moved to computer networks and virtual spaces. Technological changes have increased enterprises' development potential, but also raised the number and degree of risks. The already known threats (phishing, pharming, DDoS attacks, brute force attacks, bots and Trojans, ransomware) have been joined by new ones with AI development, often being modifications or enhancements to existing ones. These include, among others: telephone bots, deepfakes, GPT chat, fake news, data theft and system hacking. To ensure the safety and effective use of AI, these risks must be considered when developing a cybersecurity strategy.

Awareness among organizational executives about both the benefits and risks of using digital tools is growing every year. This is confirmed by data from KPMG reports in recent years. Indeed, in 2023, 15% of companies in Poland were using AI technology, and 13% planned to implement it by the end of the year (KPMG, Microsoft, 2023). By 2024, one-third of companies stated they would implement digital tools, and an additional 30% indicated they would do so soon (KPMG, Microsoft, 2024). As more organizations invest in digital technologies, concerns about their potential misuse also increase. The “Power of AI” report shows that 42% of respondents are concerned about the lack of adequate protection against cyber attacks that could disrupt AI or allow unauthorized access to sensitive data. Simultaneously, up to 30% of enterprises are not taking any special measures to prepare them for possible AI system failures (BUZZcenter, 2024).

In SMEs, implementing AI-based solutions and protecting against cyber threats is more challenging than in large organizations. Effective cybersecurity management is crucial in a rapidly changing environment where digital technologies play a significant role, regardless of the size of operations. It is essential for maintaining the integrity, confidentiality, and availability of data, which is vital for the organization's stability and security. Cybercriminals are developing increasingly sophisticated attack methods, and their activities are increasingly targeting the small business sector. Smaller business units typically have limited resources to provide effective cyber protection. Therefore, the implementation of technological security measures alone proves to be insufficient. It is necessary to adopt

a comprehensive approach to cybersecurity that considers not only technological aspects but also the organizational and human factors that are crucial to effectively countering threats.

As part of European Cyber Security Month 2024, recommendations have been made for representatives of the SME sector on what measures to take to protect the company from cyber attacks. These include (European Commission, 2024):

- increase education and deepen employee awareness,
- software update,
- setting strong passwords and two-factor authentication,
- regular backups and safe storage,
- implementing a security policy that regulates technology use, and data access, outlines procedures for security breaches,
- cooperation with experts specializing in cybersecurity.

Despite concerns, using AI by SMEs does not have to involve large expenditures, due to:

1. availability of ready-made solutions - today's market offers many ready-made AI-based tools and platforms that are available in subscription or "as-a-service" models (Creativa, 2024; Symfonia, 2024),
2. AI cloud services - enterprises pay only for the resources consumed, allowing them to scale services according to their needs and budget capabilities (Biznes.gov.pl, 2024; Vestigio, 2024),
3. process automation (Let's automate, 2025; Symfonia, 2024),
4. open-source solutions - there are many free and open-source AI tools and libraries (DigitalOcean, 2025),
5. implementation simplicity (Antczak, 2024),
6. training and educational resources availability (Portal Sztucznej Inteligencji, 2025b; Microsoft, 2024).

With these capabilities, SMEs can deploy AI solutions more cost-effectively (less costly) and more easily, making the technology more accessible to businesses with limited resources, while also enabling protection against cybercrime.

4. Research methodology

The survey was conducted based on a procedure consisting of several stages. Firstly, a comprehensive review of the literature regarding the use of artificial intelligence in business management, with an emphasis on cybersecurity aspects, was conducted. The following steps identified the research problem, posed research questions, and formulated hypotheses.

The research problem is the following: What are the existing practices, challenges and gaps in small enterprise cybersecurity management efforts? Three research questions were formulated:

1. What steps small enterprises are taking to protect themselves from cybersecurity incidents?
2. What are the barriers to managing cybersecurity in small enterprises?
3. What are the most relevant activities in the context of improving cybersecurity management in small enterprises?

The research's main objective was to analyze and assess the practices, challenges and gaps in the area of cybersecurity management in small enterprises. The following hypotheses were formulated:

- Hypothesis 1: In small enterprises, cybersecurity management activities are based on widely available solutions that do not require specialized knowledge and skills.
- Hypothesis 2: Cybersecurity management in small enterprises is most hindered by a limited investment budget and insufficient employee knowledge in the cybersecurity area.
- Hypothesis 3: Improving cybersecurity management requires implementing activities aimed at developing employees' competencies and increasing their awareness of information and communication technology's safe use.

Hypothesis testing was conducted based on a pilot study. The authors intended to verify their knowledge of the phenomenon under study and to test the research tool. The hypotheses were verified using the diagnostic survey method, a structured interview technique. The interview questionnaire contained 6 substantive questions and 3 metric questions. Respondents answered substantive questions on a five-point Likert scale. Due to the pilot nature of the study, it was conducted on a relatively small sample, 15 small enterprise owners participated in 2024. The entities represented by the respondents during the research met the criteria defined in the Act of 6 March 2018 – Entrepreneurs' Law (Dz.U. z 2024, poz. 236).

Research sample structure:

- age of the enterprise: from 1 to 5 years - 5 enterprises, from 5 to 10 years - 4, over 10 years - 5, less than one year - 1,
- place of business: city of more than 150 thousand inhabitants - 3 enterprises, city of 50 to 150 thousand - 4, city of 20 to 50 thousand - 4, city of up to 20 thousand inhabitants - 3, village - 1,
- industry: wholesale and retail trade - 3 enterprises, IT - 2, financial activities and insurance - 2, industry - 2, service activities - 6.

5. Cybersecurity in small enterprises – research results

As digital technologies rapidly evolve, cybersecurity becomes a crucial element of any organization's strategy, including those of small businesses. Growing cybercrime threats are forcing executives to take action to protect data and information systems. Investing in the employment of highly qualified professionals with the appropriate skills in this sphere is now becoming strategic for risk management in the organization. As part of the survey, respondents were asked to whom in their enterprises were entrusted with cyber security tasks. The responses obtained are as follows:

- enterprise has a dedicated cybersecurity position: 5 enterprises (33.3%),
- cybersecurity tasks are outsourced (rather sporadically): 6 enterprises (40%),
- planned to create cybersecurity specialist positions in the future: 3 enterprises (20%),
- employing such a specialist is not necessary: 1 enterprise (6.7%).

To verify hypothesis 1, respondents were asked to answer two questions. The first concerned the frequency of cybersecurity incidents. Responses were given on a scale from 1 - never to 5 - very often. The answers are presented in Table 1.

Table 1.
Frequency of appearing cyber security incidents

Rating	**1**	**2**	**3**	**4**	**5**
Number of respondents	3	4	5	2	1

Source: own elaboration.

For three enterprises (20%), cyber incidents were not reported. In nine units (60%) these events occurred infrequently (answers 2 and 3). This may indicate the presence of quite good security features. Three people (20%) gave answers 4 and 5, meaning that they often experience problems in the cybersecurity area. The vast majority of enterprises surveyed are experiencing problems related to operating in cyberspace, indicating significant challenges in protecting data and information systems.

In the second question, respondents indicated the actions they are taking to secure the company against cyber threats. The responses are presented in Table 2, where 1 means - we do not take action, and 5 - we take action constantly.

Table 2.
Actions to secure the company from cyber threats (number of respondents)

Actions	**Ratings**					**Weighted sum of ratings**
	1	**2**	**3**	**4**	**5**	
Regular updates of software and operating systems	0	1	1	7	6	63
Installation of antivirus and antimalware software	0	1	2	6	6	62
Monitoring network traffic and security events	0	1	4	5	5	59
Collaborating with cybersecurity experts	0	2	3	6	4	57
Implementation of information security policies	0	2	4	5	4	56

Cont. table 2.

Training employees on cyber security	1	2	4	5	3	52
Regular assessment of cyber security risks	1	3	5	4	2	48
Adjusting the crisis management plan for cyber security incidents	2	4	3	4	2	45
Regular use of external cyber security specialists	4	3	4	3	1	39

Source: own elaboration.

The vast majority of surveyed enterprises regularly update software and operating systems (weighted sum of ratings 63). Another activity with a similar score is the installation of antivirus and antimalware software (weighted sum of ratings 62). Quite often surveyed units monitor network traffic and security events (weighted sum of ratings 59). Enterprises are less likely to use external cybersecurity specialists (weighted sum of ratings 39). Also infrequent are activities related to correcting the crisis management plan in case of cyber incidents (weighted sum of ratings 45) and assessing cybersecurity risks (weighted sum of ratings 48). The answers obtained allow the conclusion that actions based on generally available solutions, which do not require specialized knowledge and skills, are more often taken. It is disturbing that half of the surveyed enterprises do not pay much attention to employee training in cybersecurity (7 respondents answered 1, 2, 3). This is due to both the limited ability to implement internal and external training and the owners' lack of belief in the necessity of these activities. Considering that the vast majority of those surveyed are dealing with cyberattack incidents, basing cybersecurity management strategies on publicly available solutions is insufficient. The analysis of the responses does not provide a reason to reject Hypothesis 1.

The verification of hypothesis 2 was conducted through a question regarding the degree of influence that specific barriers have on the cybersecurity management process. Respondents provided answers on a scale from 1 - no influence to 5 - significant influence (Table 3).

Table 3.
Barriers to managing cyber security in the enterprise (number of respondents)

Barriers	**Ratings**					**Weighted sum of ratings**
	1	**2**	**3**	**4**	**5**	
Limited budget for investments in cyber security solutions and tools	0	1	3	5	6	61
Threats from phishing attacks, ransomware and other malware forms	0	1	4	6	4	58
The complexity and dynamic nature of cyber threats, which are constantly evolving	0	1	6	4	4	56
The need to ensure security for remote and mobile working	0	2	5	5	3	54
Lack of resources for ongoing employee cyber security training	1	1	4	6	3	54
The need to comply with data security regulations and legal requirements (e.g., RODO, GDPR)	0	2	5	6	2	53
Lack of employee awareness of cyber threats and proper security practices	1	2	5	4	3	51
Lack of adequately trained information security specialists	0	3	6	3	3	51
Difficulty in monitoring and detecting cybersecurity incidents	0	2	7	4	2	51
Limited access to qualified cybersecurity professionals	1	2	5	4	3	51
Limited employee knowledge of new technologies and cybersecurity trends	0	3	7	3	2	49

Cont. table 3.

Lack of clearly defined policies and procedures for enterprise cyber security management	1	2	6	4	2	49
Lack of management understanding of the importance of cyber threats	3	4	3	3	2	42

Source: own elaboration.

For most enterprises, the biggest barrier is a limited budget to invest in solutions and tools to ensure effective cybersecurity management (weighted sum of ratings 61). Threats from cyber-attacks involving various forms of malware are also a significant challenge (weighted sum of ratings 58). The complexity and dynamic nature of cyber threats (weighted sum of ratings 56) make cybersecurity management quite difficult. The barriers that an overwhelming number of respondents felt were less challenging in terms of cybersecurity management were management's lack of understanding of the importance of cyber threats (weighted sum of ratings 42), lack of clearly defined related policies and procedures (weighted sum of ratings 49), and limited employee knowledge of new technologies and trends in cybersecurity (weighted sum of ratings 42). Responses analysis reveals that hypothesis 2 has been positively verified in the first part - the biggest barrier to cybersecurity management are problems related to funding cybersecurity activities. However, there are reasons to reject hypothesis 2 in its second part - limited knowledge of employees related to cybersecurity in the opinion of respondents is not a significant barrier. Representatives from 10 of the 15 enterprises indicated ratings of 2 and 3, meaning low and medium impact.

Three questions were used to verify hypothesis 3. Initially, interview participants were asked to evaluate the effectiveness of the measures the company is taking in the cybersecurity management area. The responses are presented in Table 4, where 1 means no effectiveness and 5 means very high effectiveness.

Table 4.
Effectiveness of the enterprise's cyber security management efforts

Rating	**1**	**2**	**3**	**4**	**5**
Number of respondents	1	2	7	4	1

Source: own elaboration.

Five respondents (33.3%) believe that the cybersecurity management activities undertaken at their company are highly effective (ratings 4 and 5). Seven respondents (46.6%) assessed their effectiveness at an average level (rating 3), and three respondents (20%) responded that the measures were not effective (ratings 1 and 2). The results indicate that the majority of respondents (80%) perceive cybersecurity management activities as at least moderately effective. This means there is space for improvement in enterprises to implement more effective cybersecurity strategies and tools.

Therefore, respondents were asked whether there was a need to improve cybersecurity management at their enterprises (Table 5). They gave their answers on a scale of 1 - does not need improvement, and 5 - improvement is absolutely necessary.

Table 5.
The need to improve cyber security management in the enterprise

Rating	**1**	**2**	**3**	**4**	**5**
Number of respondents	0	1	1	5	8

Source: own elaboration.

The vast majority of respondents (86.6%) recognize the need to improve cybersecurity management (ratings 4 and 5). This indicates a high risk awareness and the need for further action in this area. A small percentage of respondents (13.4%) view this need as less important, possibly due to various factors, such as the effectiveness of existing safeguards or their assessment of risk.

What actions can be most useful in improving cybersecurity management? Respondents answered this question on a scale from 1 - not very helpful to 5 - very helpful. Their opinions are presented in Table 6.

Table 6.
Assessment of actions needed to improve cyber security management at the enterprise (number of respondents)

Actions	**Ratings**					**Weighted sum of ratings**
	1	**2**	**3**	**4**	**5**	
Raising employees' awareness of safe use of information and communication technologies	0	1	3	5	6	61
Implementation of a regular cyber security training program for all employees	0	1	3	6	5	60
Implementation of technologies to protect against phishing attacks, ransomware and other threats	0	1	3	6	5	60
Creating a system of regular updates and contingency testing (e.g., backups, system recovery plans)	0	1	3	6	5	60
Implementation of tools for sensitive data encryption and communications	0	1	4	5	5	59
Regular cybersecurity reviews and audits	0	1	3	7	4	59
Updating and strengthening information security policies and internal procedures	0	1	4	6	4	58
Implementation of cyber security incident monitoring and detection systems	0	1	4	6	4	58
Establishing cyber risk management procedures and developing an incident response plan	0	1	4	6	4	58
Development and implementation of strategies to ensure security in remote and mobile work	0	1	5	5	4	57
Introducing systems to control access to data and monitor user activity	0	2	6	4	3	53
Collaboration with external information security specialists	1	2	5	5	2	50

Source: own elaboration.

Among the representatives of the surveyed enterprises (11 individuals, accounting for 73.3% of the total) believe that increasing employee awareness regarding the safe use of digital technologies is the most crucial factor (weighted sum of ratings 61). Respondents expressed a similar opinion on actions such as implementing a regular cybersecurity training program, introducing technologies to protect against cyberattacks, and creating a system of regular updates and contingency testing (in each case, the weighted sum of the ratings is 60). Slightly

surprisingly, the importance of introducing systems to control access to data and monitor user activity (weighted sum of ratings 53) and working with external information security specialists (weighted sum of ratings 50) was underestimated. Based on the feedback from respondents, activities aimed at enhancing employees' skills and awareness regarding the safe use of digital technologies are deemed necessary. Since these initiatives received the highest weighted ratings, there is no reason to reject Hypothesis 3.

6. Discussion and conclusions

The survey provided important insights into the challenges of managing cybersecurity in small enterprises. Respondents indicated several barriers, including a lack of specialized knowledge, limited financial resources, and insufficient awareness of cyber threats among employees. They evaluated the effectiveness of their enterprises' cybersecurity management at an average level. Meaning that they are aware of the need to improve activities aimed at strengthening the cyberspace operations security. The willingness to develop employees' digital competence and cybersecurity awareness can be assessed positively. The inevitable digitization of business processes and the growing complexity of cyber threats mean that enterprise digital security is no longer solely an IT specialist's domain. Increasingly, employees' decisions, habits, and levels of awareness are the organization's first and most important defense line. A significant part of security breaches are due not to advanced technical attacks, but to mistakes or employee ignorance. This indicates the importance of building cybersecurity awareness throughout the organization.

The problem for many small enterprises is IT infrastructure – from firewalls to servers and software, which has not been updated for years. Outdated solutions usually have weaker encryption mechanisms, gaps in authentication protocols and lack of manufacturer support, which significantly increases the risk of hacking and data leaks. The lack of modernization of the technical and technological environment increases the cybersecurity gap and limits the practical benefits of AI tools. Investments in hardware updates, patch management and security-by-design policies are crucial for small enterprises to be able to safely and effectively use artificial intelligence. As studies have shown, limited financial resources are a significant barrier to such modernization.

The conducted survey was a pilot and included a small respondent group, implying some limitations on the ability to generalize the results. However, the data obtained provide an important beginning point for further, more extensive analysis. During the interviews, it was noted that some questions were difficult for respondents due to the use of specialized terminology, so the survey tool should be clarified. The authors intend to conduct a broader study to identify differences in cybersecurity management depending on the enterprise's time

in the market, location, and industry. Future research will also include the possibility of evaluating the effectiveness of specific AI tools in minimizing cyber threats.

The study literature and empirical research presented showed that effective cybersecurity management in small enterprises requires a holistic approach, combining the development of digital competencies, the implementation of modern protective technologies, and the formation of a digital security culture. Small enterprise owners have a crucial role in this. They are the ones who, through their decisions and behavior, set the standards for employees. It is important to treat security as an integral part of their business processes, not as an obstacle or additional burden.

The innovative element of the presented research was the combination of two perspectives: 1) the use of AI in small enterprises and 2) cybersecurity management in this context. This allowed for a comprehensive approach to the level of awareness, practices and barriers occurring in these processes. The results of the empirical research are consistent with the conclusions drawn from the literature review. They confirm the low digital maturity of SMEs and the lack of specialist competences enabling the effective and safe use of AI tools. The information obtained is of practical and cognitive importance, as it shows real competence and organizational gaps in the small enterprise sector and indicates the need for broader support for this sector in the context of the development of digital competences and AI implementation.

References

1. AI Chamber (2024). *Rola AI w MŚP*. Retrieved from: https://aichamber.eu/report/raport-ai-chamber-2024-rola-ai-w-msp/, 28.02.2025.
2. Amoroso, E. (2006). *Cyber Security.* Summit, New Jersey, NJ: Silicon Press.
3. Antczak, J. (2024). *Wykorzystanie sztucznej inteligencji (AI) w małych i średnich firmach.* Retrieved from: https://jacekantczak.pl/wykorzystanie-sztucznej-inteligencji-%28ai%29-w-malych-i-srednich-firmach, 13.03.2025.
4. Banasiński, C., Rojszczak, M. (2023). *Cyberbezpieczeństwo. Zarys wykładu.* Warszawa: Wolters Kluwer.
5. Bielińska-Dusza, E. (2022). Transformacja technologiczna przedsiębiorstw jako skutek zastosowania sztucznej inteligencji. *Organizacja i Kierowanie, No. 1(190),* pp. 159-176.
6. Biznes.gov.pl (2024). *AI, Big Data i chmura obliczeniowa – jak nowe technologie mogą zrewolucjonizować małe i średnie przedsiębiorstwa.* Retrieved from: https://www.biznes.gov.pl/pl/portal/004811?utm_source=chatgpt.com, 14.03.2025.
7. BUZZcenter (2024). *Power of AI. Nowe możliwości rozwoju i skalowania biznesu w polskich realiach.* Retrieved from: http://buzzcenter.pl/wp-content/uploads/2024/09/RAPORT_Power-of-AI_BUZZcenter-2024.pdf, 28.02.2025.

8. Cascio, J. (2022). *Human responses to a BANI World.* Retrieved from: https://medium.com/@cascio/human-responses-to-a-bani-world-fb3a296e9cac, 13.03.2025
9. Craigen, D., Diakun-Thibault, N., Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review, Vol. 4, No. 10,* pp. 13-21.
10. Creativa. (2024). *AIaaS – czym jest sztuczna inteligencja (AI) jako usługa? AI Act i inne prawne aspekty.* Retrieved from: https://creativa.legal/aiaas-czym-jest-sztuczna-inteligencja-ai-jako-usluga/, 14.03.2025.
11. Dalenogare, L.S., Benitez, G.B., Ayala, N.F., Frank, A.G. (2018). The expected contribution of Industry 4.0 technologies for industrial performance. *International Journal of Production Economics*, *Vol. 204*, pp. 383-394.
12. Digital Sustainability Forum. (2019). *Sztuczna inteligencja jako element zrównoważonego rozwoju gospodarczo-społecznego*. Warszawa: Digital Sustainability Forum.
13. DigitalOcean. (2025). *10 open source AI platforms for innovation.* Retrieved from: https://www.digitalocean.com/resources/articles/open-source-ai-platforms, 13.03.2025.
14. IAPP Research and Insights (2023). *International Definitions of Artificial Intelligence.* Retrieved from: http://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf, 21.02.2025.
15. Jurek, M. (2023). Cyberprzestępczość w dobie transformacji cyfrowej państwa. Analiza wybranych problemów. *Transformacje*, *Vol. 1, No. 116*, pp. 45-60.
16. Kemmerer, R.A. (2003). Cybersecurity. In: *25th International Conference on Software Engineering. Proceedings* (pp. 705-715). Portland, OR: IEEE.
17. Komisja Europejska (2024). *Europejski Miesiąc Cyberbezpieczeństwa 2024: #ThinkB4UClick.* Retrieved from: https://commission.europa.eu/news/european-cybersecurity-month-2024-thinkb4uclick-2024-10-01_pl, 22.02.2025.
18. KPMG, Microsoft (2023). *Sztuczna inteligencja w firmach w Polsce: potencjał do wykorzystania.* Retrieved from: https://kpmg.com/pl/pl/home/media/press-releases/2023/07/media-press-sztuczna-inteligencja-w-firmach-w-polsce-potencjal-do-wykorzystania.html, 21.02.2025.
19. KPMG, Microsoft (2024). *Monitor Transformacji Cyfrowej Biznesu. Odkrywanie nieznanych ścieżek w cyfrowym świecie. Edycja 2024.* Retrieved from: https://kpmg.com/pl/pl/home/insights/2024/04/monitor-transformacji-cyfrowej-biznesu-edycja-2024.html, 28.02.2025.
20. Krystian, M., Zaskórski, P. (2023). Sztuczna inteligencja w usprawnianiu procesów biznesowych. *Nowoczesne Systemy Zarządzania, Vol. 18, No. 4*, pp. 15-22.
21. Kurzweil, R. (1999). *The Age of Spiritual Machines*. New York, NY: Penguin Books.
22. Let's automate (2025). *Automatyzacja i sztuczna inteligencja, czyli efektywność do kwadratu.* Retrieved from: https://www.letsautomate.pl/post/automatyzacja-i-sztuczna-inteligencja-czyli-efektywnosc-do-kwadratu, 13.03.2025.

23. Lewis, J.A. (2006). *Cybersecurity and Critical Infrastructure Protection*. Washington, DC: Center for Strategic and International Studies.
24. Microsoft. (2024). *Microsoft ogłasza inwestycję w szkolenia AI w Polsce – milion osób zdobędzie nowe kompetencje.* Retrieved from: https://news.microsoft.com/pl-pl/2024/11/28/microsoft-oglasza-inwestycje-w-szkolenia-ai-w-polsce-milion-osob-zdobedzie-nowe-kompetencje/, 13.03.2025.
25. Mieszajkina, E. (2020). *Współczesne trendy w zarządzaniu małymi przedsiębiorstwami.* Lublin: Politechnika Lubelska.
26. Mieszajkina, E., Bochen, P. (2022). Assessment of Digital Competences of Lublin Province Residents in Relational Terms. *Scientific Papers of Silesian University of Technology. Organization and Management Series, No. 166*, pp. 545-563.
27. Mieszajkina, E., Ostapińska, K. (2024). Evaluation of the Impact of the BANI World on Small Business Innovation Activities. *European Research Studies Journal, Vol. 27, No. 3*, pp. 272-288.
28. Ministerstwo Rozwoju i Technologii (2024). *Advancing the digital transformation of polish enterprises - Current State Report.*
29. Nilsson, N.J. (2014). *Principles of Artificial Intelligence*. Palo Alto, CA: Morgan Kaufmann.
30. Nowak, W. (2020). Specyfika zagrożeń w cyberprzestrzeni. In: C. Banasiński, M. Rojszczak (Ed.), *Cyberbezpieczeństwo* (pp. 145-168). Warszawa: Wolters Kluwer.
31. Ottis, R., Lorents, P. (2011). Cyberspace: Definition and implications. *5th European Conference on Information Management and Evaluation, ECIME*, pp. 267-270.
32. PBSG. (2021). *Typy cyberataków, które zagrażają bezpieczeństwu w firmach.* Retrieved from: https://www.pbsg.pl/typy-cyberatakow/, 28.02.2025.
33. Portal sztucznej inteligencji (2025a). *Czym jest sztuczna inteligencja.* Retrieved from: https://www.gov.pl/web/ai/czym-jest-sztuczna-inteligencja2, 02.03.2025.
34. Portal sztucznej inteligencji (2025b). *Programy wdrożeniowe.* Retrieved from: https://www.gov.pl/web/ai/programy-wdrozeniowe, 13.03.2025.
35. Prawo przedsiębiorców (2018). *Dziennik Ustaw Rzeczpospolitej Polskiej.*
36. PwC (2024). *Gotowi na sztuczną inteligencję*. Warszawa: PwC Polska.
37. Rich, E., Knight, K. (1990). *Artificial Intelligence*. New York, NY: McGraw Hill Science.
38. SAS (2024). *What is artificial intelligence?* Retrieved from: https://www.sas.com/pl_pl/insights/analytics/what-is-artificial-intelligence.html, 11.03.2025.
39. Schalkoff, R.J. (1990). *Artificial Intelligence: An Engineering Approach*. New York, NY: McGraw Hill College.
40. Scoutto, A.S., Miotti, M.A., Ministrero, S.G. (2021). Digital capabilities and their influence on business strategies and performance within SMEs. *Technology Analysis & Strategic Management, Vol. 33, No. 12,* pp. 1445-1459.

41. Sienkiewicz, P. (2009). Terroryzm w cybernetycznej przestrzeni. In: T. Jemioło, J. Kisielnicki, K. Rajchel (Ed.), *Cyberterroryzm – nowe wyzwania XXI wieku* (pp. 89-105). Warszawa: Akademia Obrony Narodowej.
42. Siwicki, M. (2012). Podział i definicje cyberprzestępstw. *Prokuratura i Prawo*, *No. 7-8*, pp. 45-58.
43. *Słownik języka polskiego PWN* (2025) Retrieved from: https://sjp.pwn.pl/sjp/sztuczna-inteligencja;2466532.html, 21.02.2025.
44. Symfonia (2024). *Sztuczna Inteligencja w MŚP: zastosowania, korzyści i wyzwania* Retrieved from: https://symfonia.pl/blog/finanse-i-ksiegowosc/poradnik-ksiegowej/sztuczna-inteligencja-w-msp-zastosowania-korzysci-i-wyzwania/, 14.03.2025.
45. Vestigio (2024). *Przetwarzanie w chmurze a AI – Jak sztuczna inteligencja działa?* Retrieved from: https://vestigio.agency/pl/artificial-intelligence/przetwarzanie-w-chmurze-a-ai-jak-sztuczna-inteligencja-dziala-w-srodowiskach-cloud/, 13.03.2025.
46. Wodecki, A. (2018). *Sztuczna inteligencja w kreowaniu wartości organizacji*. Kraków: Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie.
47. Wodecki, A. (2021). *Sztuczna inteligencja we współczesnych organizacjach. Jak automatyczne systemy mogą wpływać na firmy, modele biznesowe, rynki?* Warszawa: PWN.
48. Zalewski, T. (2020). *Prawo sztucznej inteligencji.* Warszawa: C.H. Beck.