European Research Studies Journal
Volume XXIX, Issue 2, 2026

pp. 595-605

The Impact of Artificial Intelligence on Organisational Security Management

Submitted 18/04/26, 1st revision 08/05/26, 2nd revision 20/05/26, accepted 29/06/26

Marta Chodyka[1], Zbigniew Ciekanowski[2], Janusz Kręcikij[3], Sławomir Wronka[4], Sławomir Żurawski[5], Barbara Drapikowska[6]

Abstract:

Purpose: *The aim of this article is to analyse the impact of artificial intelligence on organisational security management and to identify the opportunities and threats arising from the implementation of AI-based solutions in modern organisations.*
Design/Methodology/Approach: *The study employed a critical literature review, a comparative analysis, and an analysis of current reports on cybersecurity and artificial intelligence. The research process involved analysing academic publications, industry reports, and international regulations on AI governance and organisational security management. The research question was formulated as follows: how does artificial intelligence influence the effectiveness of organisational security management? The research hypothesis posited that the use of artificial intelligence enhances the effectiveness of organisational security management by improving threat identification, data analysis and the automation of incident response processes, whilst simultaneously generating new challenges related to information and organisational security.*
Findingss: *The analysis indicates that artificial intelligence significantly increases an organisation's security management effectiveness by supporting threat identification, data analysis, risk management, and the automation of security incident response. At the same time, the development of AI generates new challenges related to cyber threats, limited algorithm transparency, the phenomenon of shadow AI, data protection and the need to build effective AI governance systems.*
Practical implications: *The research findings can support organisations in building effective AI oversight systems, improving cybersecurity systems and increasing organisational*

[1]*John Paul II University in Biała Podlaska, Poland, ORCID: 0000-0002-8819-2451*
e-mail: m.chodyka@dyd.akademiabialska.pl;
[2]*The same as in 1, ORCID: 0000-0002-0549-894X,*
e-mail: zbigniew@ciekanowski.pl;
[3]*Andrzej Frycz Modrzewski Krakow University, Poland, ORCID: 0000-0002-3077-3288,*
e-mail: jkrecikij@uafm.edu.pl;
[4]*President Stanisław Wojciechowski University of Kalisz, Poland,*
ORCID: 0000-0002-2910-4757, e-mail: s.wronka@uniwersytetkaliski.edu.pl;
[5]*The same as in 3, ORCID: 0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl;*
[6]*War Studies University, Poland, ORCID 0000-0002-6852-2791*
e-mail: bdrapikowska@o2.pl;

resilience. The article also highlights the need to implement security policies, develop staff competencies and ensure compliance with AI regulations.
Originality/Value: *The article presents a comprehensive approach to the issues linking artificial intelligence, cybersecurity and organisational management. The value of the study lies in identifying the benefits and risks associated with the use of AI in organisational security systems, drawing on current international reports, academic literature, and contemporary management challenges.*

Keywords: *Artificial intelligence, cybersecurity, organisational security, AI governance, risk management*

JEL Codes: *O33, M15, D83, L23, C88.*

Paper type: *Research article.*

1. Introduction

The dynamic development of information and communication technologies and the ongoing digitalisation of management processes mean that modern organisations operate in an increasingly complex security environment. The growing importance of ICT systems, data processing, and digital communication simultaneously increases organisations' vulnerability to threats, in particular cyberattacks, data breaches, disinformation campaigns, and disruptions to the continuity of information systems. Consequently, organisational security has become a key element of effective management in both the public and private sectors.

In response to the growing scale and complexity of threats, organisations are increasingly using modern technologies to support security management processes. Artificial Intelligence (AI) is particularly important in this regard, as it represents one of the most significant areas of development for modern organisational and security systems. AI-based solutions enable the automation of analytical processes, rapid threat identification, anomaly detection in IT systems, risk forecasting, and support for decision-making. In practice, AI is used, amongst other things, in cybersecurity systems, user behaviour analysis, security monitoring, data protection and incident management.

At the same time, the development of artificial intelligence generates new challenges and threats for organisations. The use of AI can lead to new forms of cyberattacks, information manipulation, the creation of deepfake content, and an increased risk of organisations becoming dependent on digital technologies. Ethical and legal issues, as well as accountability for decisions made by systems that use artificial intelligence algorithms, remain significant concerns.

Consequently, managing an organisation's security now requires not only the implementation of modern technologies, but also the development of appropriate procedures, staff competencies and systems to oversee the use of AI.

2. Artificial Intelligence as an Element of the Modern Organisational Management System

Modern organisations operate in a dynamic technological environment, which influences how business processes, information security, and strategic decision-making are managed. The ongoing digitalisation of businesses and the development of Industry 4.0 technologies mean that the use of tools based on artificial intelligence (AI) is becoming increasingly important . These technologies are becoming an integral part of modern organisational management, supporting data analysis, process automation and the identification of organisational threats and risks (Omar, 2024).

The development of artificial intelligence is one of the most important drivers of transformation in modern organisations, and the application of intelligent systems extends beyond technical aspects to encompass strategic, organisational and operational management. The author points out that AI enables organisations to process information more quickly, forecast trends, and support decision-making, thereby increasing operational efficiency (Jarosz, 2023).

The literature on the subject emphasises that artificial intelligence plays a significant role in building so-called 'intelligent enterprises', whose operations are based on the use of knowledge, data and advanced analytical systems that support management (Nott, 2025). In the intelligent enterprise model, AI serves as a tool enabling the automation of organisational processes and supporting the organisation's knowledge and security management. The diagram below illustrates the role of artificial intelligence in the organisation's security management process.

Figure 1. *The role of artificial intelligence in the organisation's security management process.*

Source: *Own work.*

The growing importance of artificial intelligence also stems from the need to process the vast amounts of data generated by organisations. Solutions utilising machine learning, predictive analytics, or expert systems enable real-time data analysis, anomaly identification, and threat prediction. This enables organisations to respond more quickly to crisis situations and mitigate operational risk (Koziarki and Koziarska, 2025, p. 70).

Another key area of AI application is organisational and operational risk management. Research on the use of artificial intelligence in operational risk management indicates that AI supports organisations in identifying threats, analysing system vulnerabilities and mitigating the impact of security incidents. At the same time, it is emphasised that the effectiveness of AI implementation depends on the level of organisational readiness, security culture and employee competence (Ahmed and Szczepański, 2023, p. 11). The table below presents examples of AI applications within an organisation.

Table 1. *Examples of AI applications within an organisation.*

Area of the organisation	**AI application**	**Effect**
Cybersecurity	Incident detection	Faster response
Risk management	data analysis	loss mitigation
Staff management	behavioural analysis	improving efficiency
Monitoring	image analysis	Enhanced security
Data protection	Anomaly detection	risk reduction

Source: *Own work.*

The development of artificial intelligence is also changing the way personnel are managed and work is organised. Increasing attention is being paid to the importance of so-called algorithmic management, in which AI systems support action planning, employee performance assessment and decision-making processes within an organisation. The use of AI in organisations is leading to the emergence of a new model of human-technology collaboration, referred to as human-AI symbiosis, in which artificial intelligence does not replace humans but supports them in carrying out complex organisational processes.

As artificial intelligence develops, the importance of standardising the processes related to its use in organisations is also growing. The response to the need to create safe and responsible AI systems is the ISO/IEC 42001:2023 standard, which is the first international standard for an artificial intelligence management system (Biroğul, Şahin, and Esgərli, 2025). This standard sets out requirements for the implementation, monitoring and improvement of AI systems in organisations, taking into account aspects of security, accountability and risk management.

Modern organisations are also increasingly using artificial intelligence in cybersecurity (Ciekanowski *et al.,* 2024). Research indicates that AI enables the

automation of threat monitoring, incident detection and the analysis of IT system vulnerabilities. AI technologies reduce response times to security incidents and increase the effectiveness of data protection and an organisation's digital infrastructure (Achuthan, Ramanathan, Srinivas, and Raman, 2024).

Despite the numerous benefits of artificial intelligence, the literature also highlights barriers to its implementation. The most significant of these include high implementation costs, a lack of appropriate digital skills, issues related to algorithm transparency, and ethical and legal concerns. The importance of fostering an organisational culture that supports the safe and responsible use of AI technologies is also emphasised.

3. The Use of Artificial Intelligence in Organisational Security Management

Modern organisations are increasingly using AI-based solutions in security management processes. The development of digital technologies, the rise in cyber threats, and the need to respond quickly to incidents mean that traditional methods of protecting information and organisational infrastructure are proving insufficient.

Artificial intelligence enables the automation of security processes, the analysis of large datasets, and the identification of threats in real time, thereby significantly increasing the effectiveness of an organisation's security systems (Laudicella, Carboni, De Vittor, Whitfield, Doherty, and Hughes, 2025).

One of the most important areas of AI application in organisational security is cybersecurity. Systems utilising machine learning and behavioural analysis enable the detection of unusual user activity, the identification of intrusion attempts, and the analysis of IT system vulnerabilities. The literature indicates that the use of AI enables a significant reduction in the time required to identify security incidents and mitigates the effects of cyberattacks through automated responses to threats.

The growing importance of artificial intelligence is also evident in organisational risk management processes. Organisations use AI systems to analyse operational data, forecast potential threats, and support security-related decision-making. Using predictive algorithms enables earlier threat identification and the development of measures to minimise the risk of security incidents. According to research by authors specialising in AI in risk management, these solutions enhance an organisation's resilience to crises and operational disruptions (Ciekanowski *et al.,* 2024).

Artificial intelligence is also used in organisational security monitoring systems. Solutions utilising image analysis and pattern recognition are employed, for example, in video surveillance systems, access control and the protection of critical infrastructure. AI systems enable the automatic detection of dangerous behaviour, the analysis of people's movements, and the identification of situations that may pose a threat to the organisation's security.

It is noted that integrating AI with monitoring systems significantly increases the effectiveness of protecting organisational facilities and assets. The energy sector is a particularly important area for AI applications in critical infrastructure protection, as AI-based solutions support the management of renewable energy sources (RES), photovoltaic integration, smart grid operation, and the enhancement of national energy security (Grudniewski, 2025).

Information security management is also a key area of application for artificial intelligence. Organisations use AI systems to classify data, detect attempts at unauthorised access, and analyse threats related to information leaks (Grudniewski *et al.,* 2026). Using AI, it is possible to continuously monitor information systems and automatically detect anomalies that indicate potential data security breaches. These solutions are particularly important for organisations that process large volumes of sensitive information and personal data.

In organisational practice, generative artificial intelligence (Generative AI) is also increasingly being used to support security-related analytical and decision-making processes. Tools utilising AI language models enable the analysis of security reports, assist in creating incident response procedures, and support threat analysis. At the same time, it is emphasised that the development of Generative AI also increases the risks of creating sophisticated phishing and disinformation campaigns, as well as the automation of cyberattacks.

The importance of artificial intelligence in organisational security management is also confirmed by current industry reports. According to IBM reports, organisations that use AI solutions in cybersecurity achieve shorter incident detection times and lower costs associated with data breaches. It is noted that automating security processes and using AI analytics increases organisational security management efficiency. Selected challenges and benefits associated with the use of AI in organisations are presented below.

Table 2. *Selected challenges and benefits associated with the use of AI in organisations.*

Category	**Value**
Organisations without AI-based post-incident access control	97%
Organisations without an AI governance policy	63%
Average cost of a data breach	$4.4 million
Savings from AI in security	$1.9 million

Source: *IBM Security & Ponemon Institute (2025).*

Modern organisations are increasingly adopting AI-based solutions, yet the pace of implementing new technologies often outstrips the development of oversight and security mechanisms. This phenomenon is referred to as the ‘AI governance gap’.

According to research conducted by IBM and the Ponemon Institute, many organisations are implementing artificial intelligence systems without adequate risk and security management procedures.

The research indicates that as many as 97% of organisations that reported incidents involving artificial intelligence lacked adequate mechanisms to control access to AI systems. At the same time, 63% of organisations had not implemented formal AI management policies or procedures to address the so-called 'shadow AI', which involves the uncontrolled use of AI tools by the organisation's employees.

The report's findings also show that organisations using artificial intelligence in security systems achieved average savings of around $1.9 million compared to those not using such solutions. The average global cost of a data breach, meanwhile, stood at $4.4 million. These figures confirm that the responsible implementation of AI can enhance the effectiveness of an organisation's security management; however, the lack of appropriate oversight mechanisms significantly increases organisational risk.

However, implementing artificial intelligence in an organisation's security systems also presents several challenges. The most significant issues include ensuring the quality of data used by AI systems, mitigating the risk of erroneous algorithmic decisions, and addressing limited transparency in the operation of artificial intelligence models. The literature also emphasises the need to develop effective oversight mechanisms for AI systems and to adapt legal regulations to the dynamic development of artificial intelligence technology.

4. Threats, Challenges and Directions for the Development of Artificial Intelligence in Organisational Security

The rapid development of artificial intelligence means that AI technologies are becoming not only a tool supporting organisational security, but also a source of new threats and challenges for security management systems. With the increasing automation of organisational processes and the growing importance of digital data, organisations need to ensure adequate control over the AI systems they use.

The literature on the subject indicates that the lack of effective oversight mechanisms for artificial intelligence can lead to increased organisational risk, cyber threats, and issues related to accountability for decisions made by algorithms.

One of the most serious threats associated with the use of artificial intelligence is the development of advanced AI-enabled cyberattacks. Modern generative AI tools enable the creation of realistic content used in phishing, disinformation campaigns, and social engineering attacks. The development of deepfake technology poses a particular threat, as it enables the creation of fake audio and video that can be used to manipulate information and compromise an organisation's security.

It is noted that the use of AI by cybercriminals increases the scale and effectiveness of modern cyber threats (European Parliament, 2020).

The phenomenon of so-called 'shadow AI' also remains a significant problem, involving the uncontrolled use of artificial intelligence tools by an organisation's employees without the knowledge or consent of security departments or management. In practice, this leads to an increased risk of data leaks, breaches of information confidentiality and a loss of control over the processing of organisational data.

According to a report by IBM and the Ponemon Institute, as many as 63% of organisations lack formal AI management policies, whilst 97% of entities that have experienced AI-related incidents have not implemented appropriate access control mechanisms for systems using artificial intelligence. These figures point to a significant organisational gap in AI oversight (IBM, 2025).

The literature also highlights the problem of limited transparency in the operation of artificial intelligence systems. Advanced AI models, particularly those based on deep learning, often function as so-called 'black boxes', whose decision-making processes are difficult for users and organisations to interpret. This leads to issues with accountability for decisions made by AI systems and hinders the assessment of algorithmic correctness. In the context of organisational security, a lack of transparency can lead to erroneous decisions, algorithmic discrimination and a loss of trust in AI-based security systems.

Another challenge lies in the ethical and legal issues associated with the use of artificial intelligence in organisations. The development of AI necessitates adapting legal systems to new threats related to the protection of personal data, privacy, and accountability for the actions of autonomous systems.

The response to these challenges is the European Union's AI Act, which aims to establish a legal framework for regulating the use of artificial intelligence within the European Union. These regulations are designed to enhance the safety, transparency and accountability of AI systems used by organisations.

The development of artificial intelligence also requires upskilling for staff and management. Organisations are increasingly highlighting the shortage of specialists with expertise in cybersecurity, data analysis and AI systems management. A lack of appropriate digital skills may limit the effectiveness of implementing modern security technologies and increase an organisation's vulnerability to cyber threats.

It is noted that building a culture of digital security and developing staff skills are among the key elements of effective organisational security management in the age of artificial intelligence (artificialintelligenceact.eu).

Despite numerous threats, the development of artificial intelligence also presents significant opportunities to improve an organisation's security systems. In the future, the development of explainable AI (XAI) systems will take on particular importance, enabling the explanation of algorithmic decision-making processes and increasing the transparency of security systems' operations.

The integration of AI with zero-trust architecture solutions, behavioural analysis systems and the automation of security incident response processes will also play an increasingly important role. It is suggested that the future of organisational security management will be based on the synergy between human expertise and intelligent systems supporting analytical and decision-making processes (CISA, 2025).

In light of this, organisations should aim to build comprehensive AI governance systems encompassing security policies, risk management procedures, access control systems, and mechanisms for overseeing the use of artificial intelligence. It is also crucial to develop employees' digital skills, implement security standards, and ensure that the AI systems used comply with applicable legal regulations and ethical principles.

5. Conclusion

The rapid development of artificial intelligence is driving significant changes in how modern organisations operate and manage security. AI technologies are increasingly becoming an integral part of organisational systems, supporting processes such as data analysis ( ), threat identification, risk management and response to security incidents.

The use of artificial intelligence enables the automation of many processes related to the protection of information and organisational infrastructure, thereby increasing an organisation's operational efficiency and resilience to modern threats.

The analysis indicates that artificial intelligence is playing an increasingly significant role in cybersecurity, security monitoring, data protection, and decision-making support. Solutions utilising machine learning, behavioural analysis or generative artificial intelligence enable organisations to identify threats more quickly and mitigate the effects of security incidents more effectively. At the same time, the implementation of AI helps reduce costs associated with security breaches and improve organisational management efficiency.

However, the analysis confirms that the development of artificial intelligence also poses new threats and challenges to organisational security. Of particular significance are the lack of appropriate oversight mechanisms for AI, limited transparency into algorithms, the risk of AI being used in cyberattacks, and the phenomenon of shadow AI. Ethical and legal issues, as well as the need to ensure that employees and management possess the necessary digital skills, also remain significant challenges.

The above considerations lead to the conclusion that the effective use of artificial intelligence in organisational security management requires the implementation of comprehensive AI governance systems encompassing risk management procedures, security policies, access control mechanisms, and systems for overseeing the technologies in use. Building a culture of organisational security and developing competencies in the safe use of artificial intelligence are also key.

The results obtained confirm the research hypothesis that artificial intelligence enhances the effectiveness of organisational security management by improving threat identification, data analysis and the automation of incident response processes, whilst simultaneously generating new challenges related to information and organisational security.

In the future, the development of artificial intelligence is likely to lead to further transformation of organisations' security systems, and the effectiveness of security management will increasingly depend on the organisation's ability to integrate modern AI technologies with appropriate oversight mechanisms, legal regulations and staff competencies.

References:

Achuthan, K., Ramanathan, S., Srinivas, S., Raman, R. 2024. Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. Front Big Data, 7, 1497535.

Ahmed, M.F., Szczepański, M. 2023. The factors disrupting the evolution of artificial intelligence in operational risk management in the Bangladeshi IT sector – A case study. Scientific Journals of Poznań University of Technology.

Artificial Intelligence, CISA. https://www.cisa.gov/ai.

Biroğul, S., Şahin, Ö., Esgərli, H. 2025. Exploring the Impact of ISO/IEC 42001:2023 AI Management Standard on Organisational Practices. Advances in Artificial Intelligence Research, 5(1), 14-22.

Ciekanowski, M., Żurawski, S., Pauliuchuk, Y., Ciekanowski, Z., Marciniak, S. 2024. Strategies for Effective Cybersecurity Management in Organizations. European Research Studies Journal, Volume XXVII, Issue 1, 365-379.

Ciekanowski, Z., Gruchelski, M., Nowicka, J., Zdunek, M., Żurawski, S. 2024. Risk Management and Organizational Resistance to Threats. European Research Studies Journal, Volume XXVII, Issue 1, 142-153.

EU Artificial Intelligence Act, Up-to-date developments and analyses of the EU AI Act, https://artificialintelligenceact.eu/.

European Parliament. What is artificial intelligence and how is it used? https://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used?

Grudniewski, T., Chodyka, M., Ostrowska, M., Ciekanowski, Z., Elak, L., Kuznetsov, V., Zamiar, Z. 2026. The Role of Artificial Intelligence in Cybersecurity Management in the Public Sector. European Research Studies Journal, Volume XXIX, Issue 2, 121-133.

Grudniewski, T. 2025. Integracja fotowoltaiki wspieranej sztuczną inteligencją w strategiach bezpieczeństwa energetycznego państw (Integration of AI-Supported Photovoltaics in National Energy Security Strategies), in Wielowymiarowość środowiska bezpieczeństwa. Część pierwsza (Multidimensionality of the Security Environment. Part One), ed. Dariusz Brążkiewicz, Marta Chodyka, Tomasz Grudniewski, and Julia Nowicka (Biała Podlaska: John Paul II University in Biała Podlaska), 227-249. https://doi.org/10.29316/9788368103199_12.

IBM, Cost of a Data Breach Report 2025.

Jarosz, S. 2023. Artificial Intelligence – an agenda for management sciences. E-mentor, 2(99), 47-55.

Koziarski, M., Koziarska, S. 2025. Artificial intelligence in crisis management: enhancing organisational resilience through intelligent systems. Humanitas Zarządzanie, 26(4), 67-76.

Laudicella, V.A., Carboni, S., De Vittor, C., Whitfield, P.D., Doherty, M.K., Hughes, A.D. 2025. Integration of Global Lipidomics and Gonad Histological Analysis via Multivariate Chemometrics and Machine Learning: Identification of Potential Lipid Markers of Ovarian Development in the Blue Mussel (Mytilus edulis). Lipidology, 2, 5.

Nott, C. 2025. Organisational adaptation to generative AI in cybersecurity: A systematic review. arXiv. https://arxiv.org/abs/2506.12060.

Omar, M. 2024. Integrative approaches in cybersecurity and AI. arXiv. https://arxiv.org/abs/2408.05888.