European Research Studies Journal
Volume XXVII, Issue 3, 2024

pp. 765-777

Managing Organizational Security in the Context of Global Challenges

Submitted 04/07/24, 1st revision 29/07/24, 2nd revision 22/08/24, accepted 30/09/24

Aneta Chrząszcz[1], Marek Ciekanowski[2], Sławomir Żurawski[3], Wiesława Załoga[4], Sylwester Pietrzyk[5]

Abstract:

Purpose: *The aim of the article is to analyse strategies and methods for managing security in organizations, with a particular focus on their adaptation to global challenges. The article aims to identify best practices and develop recommendations for organizations to effectively respond to threats and maintain operational stability.*

Design/Methodology/Approach: *The research problem was formulated as follows: How can organizations effectively manage security to minimize risk and maintain operational continuity in the face of global challenges? Corresponding to the research problem, the research hypothesis was formulated: Organizations that integrate modern approaches to security management, considering global challenges, are more resilient to disruptions and better prepared to respond to threats. Appropriate research methods were used, including a review of current scientific research and publications related to security management and global challenges, as well as the use of the latest research presented in documents and reports on cybersecurity published between 2020 and 2024 by international organizations. A systemic analysis was conducted by assessing how different elements of security management are integrated and how they impact organizational resilience.*

Findings: *A key task for contemporary organizations is to identify and analyse global trends and potential threats that may affect their operations. Understanding these challenges allows for the development of risk management strategies that can minimize potential damage. In this context, international cooperation, information exchange, and the implementation of best practices in security also become crucial.*

Practical implications*: Effective adaptation to long-term security challenges requires a comprehensive approach that includes anticipating the evolution of threats, developing a strong security culture, analysing future scenarios, and investing in research and innovation.*

[1]*Faculty of Economics, John Paul II University in Biala Podlaska, Poland, ORCID: 0000-0001-9749-274X, aneta.chrzaszcz@op.pl;*
[2]*University of Social Sciences, Poland, ORCID: 0009-0009-1271-0652, marek@ciekanowski.pl;*
[3]*State School of Higher Education in Chełm, Poland, ORCID: 0000-0001-9527-3391, slawomir.zurawski@onet.pl;*
[4]*Military University of Technology, Warsaw, Poland, ORCID 0000-0001-7758-0187, wieslawa.zaloga@wat.edu.pl;*
[5]*Warsaw Management University, Poland, ORCID: 0000-0001-7697-0853, spietrzyk16@gmail.com;*

Organizations that implement these strategies will be better prepared to manage risk and adapt to a dynamically changing global environment.
Originality/Value: *Contemporary organizations operate in an increasingly complex and unpredictable environment, where global challenges such as climate change, pandemics, cyber threats, political instability, and globalization significantly impact their functioning. The article provides both theoretical frameworks and practical guidelines for managing organizational security in the context of a dynamically changing global environment.*

Keywords: *Security, management, organization, technology, transformation.*

JEL: *M14, L15.*

Paper type: *Research article.*

1. Introduction

In today's rapidly changing world, organizations around the globe face increasingly complex and diverse security challenges. Globalization, rapid technological advancements, climate change, and unstable geopolitical situations create an environment where threats can emerge from various, often unpredictable, sources. In this context, managing organizational security becomes a crucial element for ensuring survival and success.

Organizational security is no longer just about protection from traditional threats such as theft or physical attacks. In the face of global challenges such as cyberattacks, terrorism, pandemics, and climate change, a holistic approach to security is necessary. This approach includes both physical and digital aspects, as well as human and organizational factors.

A key task for contemporary organizations is to identify and analyse global trends and potential threats that may impact their operations. Understanding these challenges enables the development of risk management strategies that can minimize potential damage. In this context, international cooperation, information exchange, and the implementation of best practices in security also become essential.

2. Identification of Global Challenges Affecting Organizational Security

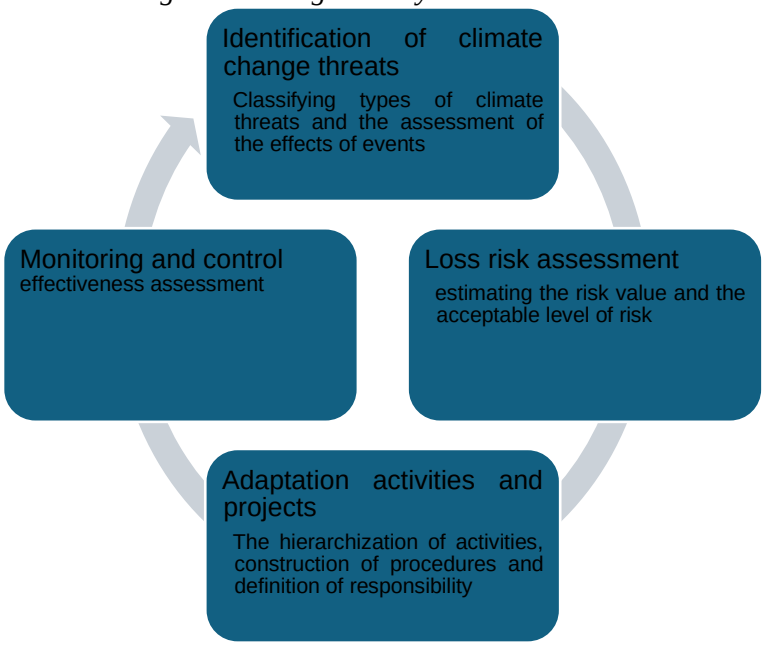
Climate change represents one of the most pressing challenges for contemporary organizations, affecting nearly every aspect of their operations. Adaptation plans for climate change are a direction of responsibility for the socio-economic impacts resulting from the consequences of climate change (Lorek, 2023). Extreme weather events, such as hurricanes, floods, wildfires, and prolonged droughts, are becoming more frequent and intense, which directly threatens the physical security of

organizational infrastructure, human resources, and supply chains (Sixth Assessment Report (AR6), IPCC). For example, manufacturing facilities may be destroyed by floods, leading to prolonged downtime and financial losses. Conversely, droughts can affect the availability of raw materials, disrupting production processes and potentially increasing operational costs (Klein *et al.*, 2003).

Rising sea levels are another serious threat, especially for organizations located in coastal areas (https://www.mckinsey.com/capabilities/sustainability/our-insights/climate-risk-and-response-physical-hazards-and-socioeconomic-impacts).

Coastal flooding can lead to building damage, property loss, and the need to evacuate personnel. Long-term changes, such as coastal erosion and soil salinization, may require costly investments in infrastructure adaptation or even relocating operations to safer locations. Below is a diagram illustrating a sample climate change risk management cycle.

Figure 1. *Climate change risk management cycle – own elaboration.*



Source: *Lorek, 2023.*

Climate change also affects the socio-economic stability of the regions in which organizations operate. Intensifying climate crises can lead to population migration, increased social and political tensions, and disruptions in local markets (Stern, 2007; Grima *et al.*, 2023). All of this creates an unstable environment where conducting business becomes challenging, and the risk of disruptions increases.

For organizations, climate change means not only responding to current threats but also engaging in long-term planning and adaptation (Thalassinos *et al.,* 2023). Investing in sustainable technologies, developing climate risk management plans, and participating in initiatives aimed at mitigating the effects of climate change become essential. Organizations must be prepared for the impact of climate change on their operations in ways that may have previously been difficult to predict, requiring flexibility, innovation, and a strategic approach to security management.

Pandemics and global health crises, such as COVID-19, also have a significant impact on organizations worldwide. The COVID-19 pandemic highlighted the fragility of global supply chains and organizations' ability to quickly respond to unforeseen disruptions. Many companies faced sudden production halts, raw material shortages, and distribution disruptions, leading to significant financial and operational losses (McKinsey & Company, 2020).

Global health crises force organizations to adapt to new working conditions, including remote work and the implementation of advanced digital technologies. Organizations had to rapidly adjust their operational strategies to ensure business continuity while also safeguarding the health and safety of their employees. Implementing flexible working hours, investing in IT infrastructure, and developing health policies became essential elements for survival during the crisis.

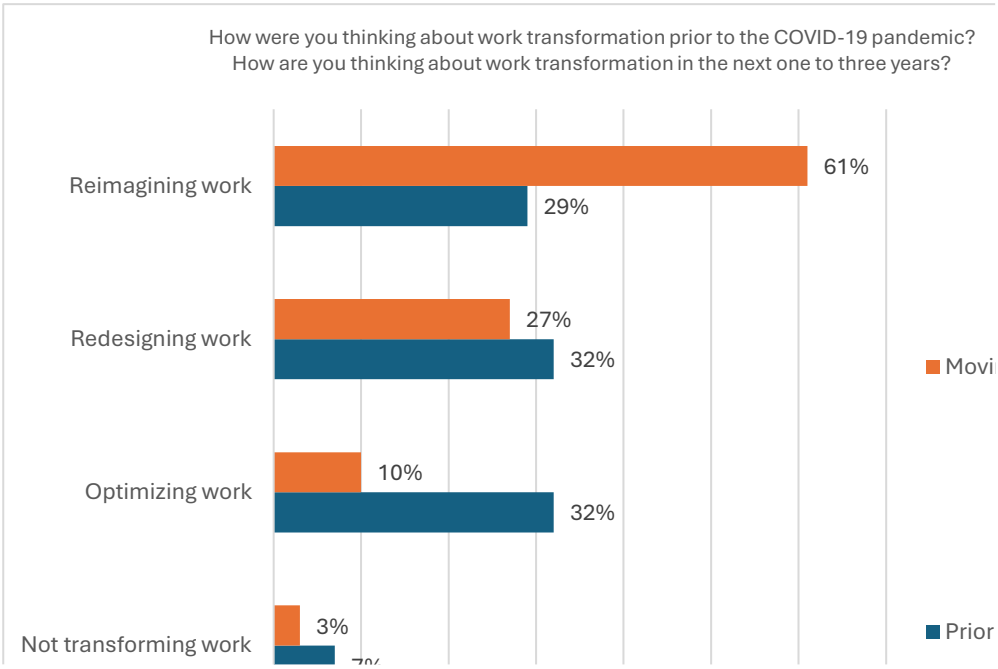
The pandemic also accelerated the need for crisis management plans and resilience strategies (Global Human Capital Trends 2021, Deloitte). Organizations that had not previously developed such plans had to quickly adapt to the dynamically changing situation (World Economic Forum – The Future of Jobs Report 2020).

Many companies invested in developing new business models that allowed for better preparation for future health crises and other unforeseen global events. Below are responses from Deloitte's survey on managers' approaches to work before and during the COVID-19 pandemic, indicating a shift in focus from optimizing work to changing it.

Additionally, the COVID-19 pandemic has highlighted the importance of international cooperation and information exchange between organizations and governments in the field of public health. A lack of coordinated response to the crisis can lead to severe consequences, such as uncontrolled disease spread, which in turn impacts the stability of global markets and the security of organizations worldwide (WHO COVID-19 Response 2021, World Health Organization).

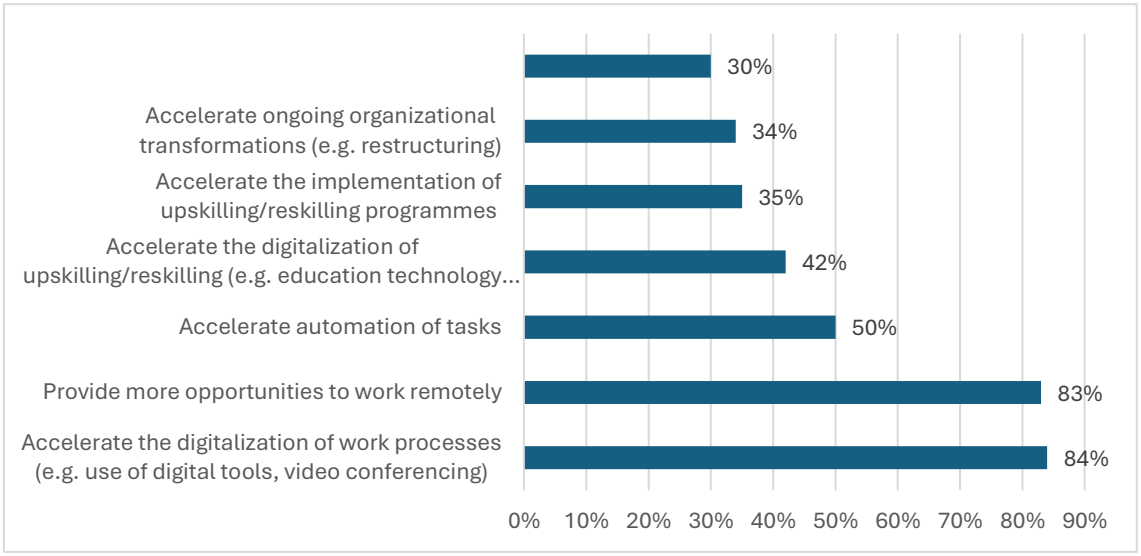
The Future of Jobs Survey 2020 report outlines planned adjustments in business operations in response to COVID-19. The most important of these are presented in Figures 2 and 3.

Figure 2. *Executives are shifting their focus from optimizing work to reimagining work.*



Source: *The 2021 Deloitte Global Human Capital Trends survey.*

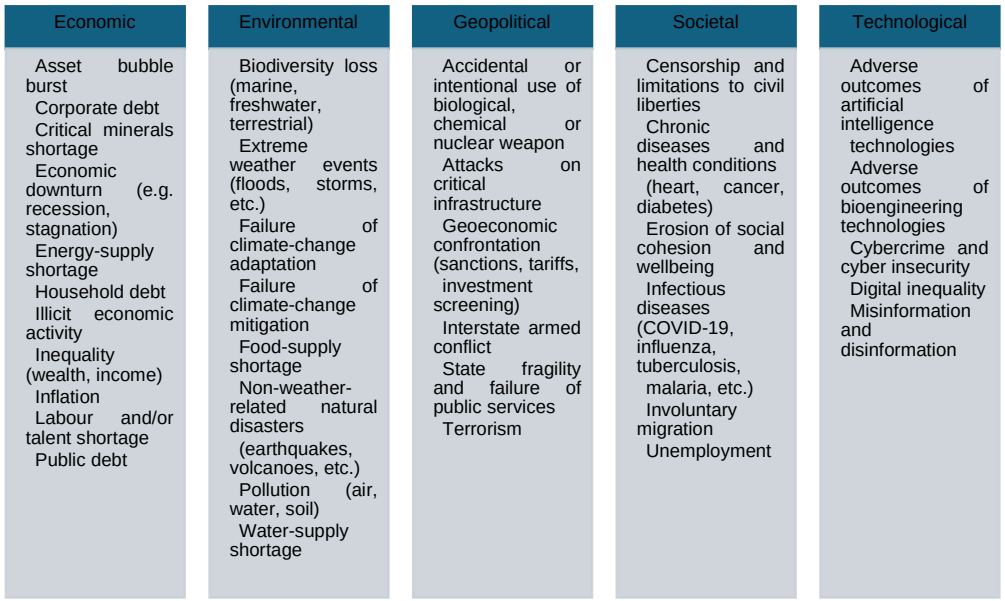
Figure 3. *Planned business adaptation in response to COVID-19.*



Source: *Future of Jobs Survey 2020, World Economic Forum.*

In the 2024 World Economic Forum Executive Opinion Survey 2023 report, a list of risks is presented, categorized by type. The following diagram shows a list of 36 risks included in the World Economic Forum's Executive Opinion Survey (EOS) 2023, conducted from April to August 2023. The risks are comparable to those in the Global Risks Perception Survey (GRPS) but are applied at a more detailed level to reflect potential short-term and national manifestations of global risks (World Economic Forum Executive Opinion Survey 2023) (Figure 4).

Figure 4. *National risk list.*



Source: *World Economic Forum Executive Opinion Survey 2023.*

The COVID-19 pandemic has had a significant impact on the global economy. Due to border closures, international economic exchange has decreased. Furthermore, the activity of most industries has slowed down (Czajkowska, 2020), and organizations have had to adapt to major changes.

The emergence of COVID-19 and its rapid global spread initiated and forced many organizations to alter their structures and directions toward digitization and increased resilience against cyber threats (Ciekanowski *et al.*, 2023).

The rise in cyberattacks and the development of organized crime at a global level pose a serious threat to data security and organizational operations. As digital technologies become more advanced, cybercriminals are using new techniques to breach security and steal sensitive information. Attacks such as ransomware,

phishing, and advanced persistent threats (APT) are becoming more common, leading to serious financial and operational consequences for affected organizations.

Cybercrime, often operating within international criminal groups, is increasing the scale and intensity of attacks. These groups use sophisticated techniques, including social engineering and advanced spyware, to compromise organizational systems, leading to data theft, privacy breaches, and the disruption of business operations. Examples such as attacks on the healthcare sector during the COVID-19 pandemic illustrate the severe impacts of cyber threats on critical infrastructures.

The rise in cyber threats forces organizations to invest in modern security technologies and develop risk management strategies. Implementing advanced incident detection and response systems, regularly testing security measures, and training employees in cybersecurity are essential to minimizing risk and protecting against potential attacks. Organizations must also be prepared to respond quickly to incidents and collaborate with law enforcement and other entities to effectively counter organized crime.

The long-term consequences of cyber threats include not only financial losses but also damage to reputation and customer trust. The evolution of threats requires continuous adaptation by contemporary organizations. Regularly increasing employee awareness is a fundamental safeguard that helps minimize the occurrence of threats (Szafranek, 2021). Organizations that fall victim to cyberattacks may face prolonged issues in managing their image and customer relations, which can affect their competitiveness and market stability.

Globalization is another factor causing significant changes in organizational operations. Globalization, as a phenomenon of increasing integration of economies and societies worldwide, introduces organizations to new, often unfamiliar operational conditions. On the one hand, globalization creates tremendous opportunities for market development, increased efficiency, and cost optimization. On the other hand, it also introduces new risks associated with political unpredictability and changing geopolitical environments, which can significantly impact operational and strategic security. The table below presents the benefits and risks associated with globalization.

The diversity of solutions proposed today by management, as well as the rapid globalization of the economy, and in particular the dynamic development of new technologies, mean that the management of a 21st-century enterprise must be oriented towards the external environment of that enterprise (Szymańska, 2012).

Political unpredictability, including instability of governments, international conflicts, and changes in trade policy, are becoming increasingly serious threats to global business operations. The rise in geopolitical tensions, such as trade wars or economic sanctions, can lead to disruptions in supply chains, increased costs, and

market uncertainty. An example is the recent changes in trade policy between the USA and China, which had a significant impact on international trade and market stability.

Table 1. *Benefits and threats associated with globalization*

Benefits of globalization	Threats of globalization
● brings culturally and geographically distant countries closer together; ● promotes the exchange of information, ideas, and concepts; ● supports the dissemination of better, more efficient, energy-saving, and eco-friendly technologies; ● accelerates the transfer of developmental factors; ● promotes competition; ● increases investments in economically attractive regions; ● disseminates knowledge; ● economically activates countries that are beneficiaries of direct investments; ● integrates and creates a platform for cooperation among people from different cultural areas; ● strengthens the processes of democratization.	● means the economic expansion of multinational and transnational corporations; ● makes it impossible to control corporations that follow their own economic logic; ● weakens the position of the state and forces the creation of conditions favourable to investment and retention of corporate capital; ● weakens the role of the state in underdeveloped countries; ● disseminates culturally foreign models; ● multiplies the cultures of transnational corporations; ● temporarily exploits economic factors (low wages, low prices of raw materials and energy carriers, legal and tax conditions); ● complicates the oversight of corporations by state regulatory institutions through the use of their own internal work systems; ● entails an intensive process of production, distribution, information, financial, and capital linkages created and controlled solely by corporations in the global market.

Source: *Czaja, 2001.*

Organizations must adapt their operational and strategic strategies to growing geopolitical risks by developing flexible and resilient business models. It is crucial to implement effective risk management strategies that take into account changing political and economic conditions. Examples of such strategies include the diversification of suppliers, the development of local supply chains, and adaptation to changing regulations and trade policies.

Long-term planning and a strategic approach to managing geopolitical risk are becoming essential for ensuring operational and strategic security. Organizations should invest in geopolitical analysis, risk monitoring, and building relationships with key stakeholders to effectively respond to changing conditions and minimize potential threats.

In summary, global challenges such as climate change, pandemics, cyber threats, and geopolitical risks have a significant impact on organizational security. Each of these areas introduces unique risks that require appropriate management and adaptation to

ensure the stability and continuity of operations in an increasingly complex and unpredictable global environment.

3. Security Management Strategies

Proactive risk management is a key element of the security strategy, which involves identifying, analysing, and managing risks before they materialize. Organizations should use a systematic approach to assess risks related to global challenges in order to minimize their negative impacts. This process includes several key steps: identifying potential threats, assessing their likelihood and potential consequences, and developing mitigation strategies.

Tools such as risk mapping, scenario analysis, and Business Impact Analysis (BIA) are essential for effective risk management. For example, in the context of climate change, organizations may conduct a risk assessment related to extreme weather events and adjust their operational strategies to minimize the impact of these threats on their activities.

Business Continuity Management (BCM) is a crucial strategy that ensures organizations can continue operations even in the face of serious disruptions. BCM involves integrating prevention, response, and recovery plans to minimize the impact of global events on organizational operations.

An additional benefit of BIA is the ability to determine the timing of the threat and its scope of impact on various subsystems of the organization. The analysis of the weight of losses allows for the division of events and situations into critical (those with significant consequences for the organization) and non-critical (those with less importance for the business) (Starosta, 2016, p. 486).

Within BCM, organizations should develop detailed emergency plans that account for various disruption scenarios, such as pandemics, natural disasters, or cyberattacks. Planning should include identifying key functions and processes, establishing critical resources, and procedures for restoring operations. Regular testing of plans and staff training is essential to ensure the effectiveness of BCM strategies in practice.

Globalization and the development of information technologies cause significant changes in the business environment and consequently in the organizations themselves, which must adapt to these changes (Pens-Pietrzak, 2016). Modern technologies play a key role in enhancing organizational security; thus, they are a crucial element in organizational security management, especially in the context of global challenges. Below is how technology can support security:

- Artificial Intelligence (AI): AI can assist in automating data analysis and threat identification. Machine learning algorithms can detect anomalies and

potential threats before they become serious problems (Przegalińska, Jemielniak, 2023);

- Blockchain: Blockchain technologies can ensure data and transaction security by ensuring their integrity and immutability;
- Big Data and analytics: Big data analytics tools allow for processing large amounts of information to identify trends and threats. Data analysis can provide valuable insights into potential risks and support real-time decision-making.

International cooperation and cross-sector partnerships are crucial in managing global security. Organizations should collaborate with other companies within their industry to jointly develop risk management strategies and share knowledge. These partnerships may include cooperation on security standards, research and development, and sharing information about threats. Collaboration with governments and regulatory agencies allows for a better understanding of legal and regulatory requirements and effectively adjusting organizational actions to the changing regulatory environment.

4. Adaptation and Long-Term Challenges for Organizational Security

In the third part of the article, the authors focus on the long-term challenges facing organizations in the face of a dynamically changing global environment. Key issues include the evolution of threats, the development of a security culture, future scenarios of global challenges, and the need for further research and innovation. As global challenges evolve and change, so does the nature of threats to organizational security.

Future threats may differ from those we observe today and may involve new areas of risk. For example, climate change may lead to an increase in the frequency and intensity of natural disasters, such as hurricanes, floods, and fires, which will have a direct impact on organizational activities.

On the other hand, technological development may introduce new types of cyber threats. Advanced attacks, such as those using artificial intelligence to bypass traditional security systems, may become more common. Furthermore, geopolitical changes and rising international tensions may introduce new risks related to supply chains and international regulations.

Organizations must monitor these changing threats and adjust their security strategies to effectively manage new risks. Cooperation with experts and participation in industry forums and research initiatives can help in identifying and anticipating future threats.

A strong security culture is crucial for effective risk management and adaptation in the face of new challenges. This culture should promote values such as

responsibility, transparency, and continuous improvement. Security culture is a phenomenon that allows individuals to achieve the following goals:

- Effective control over possible threats to the entity, resulting in an optimal level of threats at a given place and time;
- Recovery of the entity's security when it is lost;
- Optimization of the levels of the multi-sectoral development process of the security entity, aiming for harmony among security sectors in the context of the hierarchy of the entity's goals;
- Effective stimulation on a social and individual scale, awareness of the highest human need for self-improvement, and the creation of a trichotomous development—mental, social, and material—by supporting beliefs, motivation, and attitudes that strengthen individual and collective actions towards the potential of autonomous defence (self-defence) of individual and group security entities (Piwowarski, 2015).

Organizations must invest in education and training to increase employee awareness about threats and security procedures. The development of a security culture also includes promoting flexibility and readiness to adapt to changing conditions. Organizations should implement policies that encourage innovation and experimentation with new solutions in security management. Regularly updating security procedures and policies and involving employees in decision-making processes can support the development of such a culture.

Analysing possible future scenarios of global challenges is an important element in preparing organizations for unknown threats. Organizations should conduct scenario analyses that consider various possibilities for future events, such as further pandemics, climate change, or the development of new technologies.

Such analyses allow for the identification of potential risks and the development of contingency plans. Organizations should also regularly update their strategies and plans based on new information and changing circumstances. Developing "what-if" scenarios can help in preparing for unpredictable situations and enable faster and more effective responses to new challenges.

5. Conclusion

In the face of dynamic global challenges, further research and innovation are essential for effective security management. Organizations must invest in scientific research and the development of new technologies that can help in identifying and countering new threats. Collaboration with universities, research institutes, and other research organizations can contribute to the development of new solutions and strategies. Organizations should also promote a culture of internal innovation by encouraging employees to propose new ideas and improvements in security. Furthermore, continuous monitoring of trends and innovations in the field of security

management allows for rapid adaptation to the changing environment. Investments in new technologies, such as AI-based threat detection systems or advanced big data analytics, can significantly enhance an organization's ability to respond to new challenges.

In summary, the effective adaptation to long-term security challenges requires a comprehensive approach that includes anticipating the evolution of threats, developing a strong security culture, analysing future scenarios, and investing in research and innovation. Organizations that implement these strategies will be better prepared to manage risk and adapt in a dynamically changing global environment, which demonstrates that the proposed research hypothesis has been confirmed.

References:

Climate Risk and Response: Physical Hazards and Socioeconomic Impacts, McKinsey & Company. https://www.mckinsey.com/capabilities/sustainability/our-insights/climate-risk-and-response-physical-hazards-and-socioeconomic-impacts.

Ciekanowski, M., Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y., Boguski, J. 2023. The Impact of Digitalization and the COVID-19 Pandemic on Information Security Management in the Enterprise. European Research Studies Journal, Volume XXVI, Issue 3.

Czaja, I. 2001. Globalizacja, globalizm, przedsiębiorczość – szanse i zagrożenia. In: Globalizacja ISS, red. J. Klich, Kraków.

Czajkowska, A. 2020. Wpływ pandemii COVID-19 na działania CSR podejmowane przez przedsiębiorstwa. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie, 3.

Global Human Capital Trends. 2021. Deloitte. https://www2.deloitte.com/pl/pl/pages/human-capital/articles/raport-trendy-hr 2021.html.

Grima, S., Thalassinos, E., Cristea, M., Kadłubek, M., Maditinos, D., Peiseniece, L. (Eds.). 2023. Digital transformation, strategic resilience, cyber security and risk management. Emerald Publishing Limited.

Klein, R.J.T., Nicholls, R.J., Thomalla, F. 2003. Resilience to Natural Hazards: How Useful is this Concept? Global Environmental Change Part B: Environmental Hazards, Volume, 5.

Lorek, M. 2023. Zarządzanie ryzykiem zmian klimatycznych jako element bezpieczeństwa, wyzwań i odpowiedzialności. In: Zrównoważony rozwój i europejski zielony ład imperatywami doskonalenia warsztatu naukowca, red. J. Buzek, H.A. Kretek, M. Staniszewski, Wydawnictwo Politechniki Śląskiej, Gliwice.

Penc-Pietrzak, I. 2016. Zmiana paradygmatów w zarządzaniu. Zeszyty Naukowe Politechniki Łódzkiej, Organizacja i Zarządzanie, z. 65.

Piwowarski, J. 2015. Fenomen bezpieczeństwa. Pomiędzy zagrożeniem a kulturą bezpieczeństwa. Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego ”Apeiron” w Krakowie, Kraków.

Przegalińska, A., Jemielniak, D. 2023. Artificial Intelligence and Business Strategy: The Winner takes it AI. MT Biznes, Warszawa.

Risk, Resilience, and Rebalancing in Global Value Chains. 2020. McKinsey & Company. https://www.mckinsey.com/capabilities/operations/our-insights/risk-resilience-and-rebalancing-in-global-value-chains.

Sixth Assessment Report (AR6), IPCC (Intergovernmental Panel on Climate Change). https://www.ipcc-data.org/ar6landing.html.
Szafranek, D. 2021. Wpływ rozwoju cyberprzestępczości na funkcjonowanie współczesnych organizacji. Nowoczesne Systemy Zarządzania, Zeszyt 16, nr. 4.
Szymańska, A. 2012. Globalizacja a nowe koncepcje zarządzania przedsiębiorstwem. In: Rola przedsiębiorczości w edukacji, red. Z. Zioło, T. Rachwał, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie, Instytut Geografii Zakład Przedsiębiorczości i Gospodarki Przestrzennej, Warszawa-Kraków.
Starosta, A. 2016. Ciągłe doskonalenie w zarządzaniu ciągłością działania. Zeszyty Naukowe Politechniki Śląskiej. Seria: Organizacja i Zarządzanie, z. 97.
Stern, N. 2007. The Economics of Climate Change: The Stern Review. https://www.lse.ac.uk/granthaminstitute/publication/the-economics-of-climate-change-the-stern-review/.
Thalassinos, E., Kadłubek, M., Norena-Chavez, D. 2023. Theoretical Essence of Organisational Resilience in Management. In: Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 133-145). Emerald Publishing Limited.
The Future of Jobs Report. 2020. World Economic Forum.
The 2021 Deloitte Global Human Capital Trends survey.
World Economic Forum Executive Opinion Survey. 2023.
WHO COVID-19 Response. 2021. World Health Organization.