European Research Studies Journal
Volume XXVII, Issue 3, 2024

pp. 460-471

Managing Organizational Security in the Era of Digital Transformation

Submitted 22/06/24, 1st revision 14/07/24, 2nd revision 26/07/24, accepted 26/08/24

Julia Nowicka[1], Zbigniew Ciekanowski[2], Janis Kudins[3], Paweł J. Dąbrowski[4]

Abstract:

Purpose: *The article aims to analyse the management of organizational security in the context of digital transformation. It focuses on identifying key threats associated with digitization, evaluating the effectiveness of current security management methods, and highlighting areas that require further research. The goal is to demonstrate how a comprehensive and dynamic approach to security management can support organizations in fully leveraging the potential of digital transformation while minimizing risks and securing their future.*

Design/Methodology/Approach: *The article presents the essence of organizational security and analyses the management and functioning of organizations in the era of digitization. It concludes that security must be tailored to the specific characteristics of the organization and its digital environment. The main research problem is formulated as follows: How can organizations effectively manage security in the face of dynamic technological changes and increasing threats? In accordance with this research question, a hypothesis is proposed, which assumes that organizations adopting a holistic and proactive approach to security management are more effective in protecting their digital resources. The study employs appropriate research methods, including the analysis of scientific and industry literature to identify current trends, the analysis of data from reports in the studied area to identify patterns and draw conclusions, and the utilization of reliable online sources to support the research findings. This comprehensive approach aims to provide insights into how organizations can enhance their security management practices amidst the challenges posed by digital transformation.*

[1]*War Studies University, Poland, ORCID: 0000-0002-0778-0519, j.nowicka@akademia.mil.pl;*
[2]*Faculty of Economics, John Paul II University of Applied Sciences in Biala Podlaska, Poland, ORCID: 0000-0002-0549-894X, zbigniew@ciekanowski.pl;*
[3]*Daugavpils University, ORCID: 0000-0002-5870-8023, janis.kudins@du.lv;*
[4]*Warsaw Management University, Poland, ORCID: 0000-0002-3581-507X, paweljdabrowski@gmail.com;*

Findings: *Organizations should adopt a proactive approach to security management, focusing on prevention and early detection of threats rather than merely reacting after an incident occurs. Consequently, the proposed research hypothesis has been confirmed. Security must be tailored to the specific characteristics of the organization and its digital environment. Flexible and scalable security strategies enable quicker responses to changing conditions.*
Practical implications*: This article presents the main challenges associated with security management in the context of digital transformation and outlines best practices and strategies that can help organizations effectively secure their resources. It addresses issues such as the importance of a security culture within the organization, the role of modern technologies in ensuring protection, and the necessity of external collaboration in the fight against cyber threats.*
Originality/Value: *Digital transformation introduces a series of changes that revolutionize the way organizations operate and their security. The increased use of digital technologies brings significant benefits, but it also introduces new security challenges. Modern organizations must not only secure their IT systems but also adapt their approach to security management to the dynamically changing digital environment. As technology advances, new types of threats and attacks emerge. Cybercriminals are becoming increasingly sophisticated, which requires the use of advanced tools and defence methods.*

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

JEL: *M14, L15.*

Paper type: *Research article.*

1. Introduction

Digital transformation has become a key element of the development strategy of many organizations around the world. The introduction of modern technologies, such as cloud computing, artificial intelligence, big data, or the Internet of Things (IoT), enables companies to improve operational efficiency, innovation, and better understanding of customer needs. However, with the increasing degree of digitization, organizations face new challenges related to security.

Security management in the era of digital transformation is no longer limited only to traditional methods of physical or informational protection. A comprehensive approach becomes necessary, which integrates various aspects of security, such as data protection, risk management, cybersecurity, and employee education. In today's world, cyber threats are becoming increasingly sophisticated and widespread, which requires organizations to continuously monitor and adapt to changing conditions.

This article will discuss the main challenges related to security management in the context of digital transformation and present the best practices and strategies that can help organizations effectively secure their resources. Issues such as the importance

of a security culture within the organization, the role of modern technologies in ensuring protection, and the necessity of external collaboration in the fight against cyber threats will be addressed.

The goal of the article is to show how a comprehensive and dynamic approach to security management can support organizations in fully utilizing the potential of digital transformation, while minimizing risk and securing their future.

2. Organizational Security

Modern society, increasingly dependent on technology, has rising expectations regarding security in the digital context. Unfortunately, these expectations often do not keep pace with the actual capabilities to ensure security, leading to a growing gap (Ziarko, 2019; Velinov *et al.*, 2023; Tyagi *et al.*, 2023).

The crisis in the global market related to COVID-19 demonstrated how quickly situations can change, despite the absence of forecasts or warning signs. With adapting to the new circumstances, the most technologically innovative companies and industries have adapted best.
(https://www.it.integro.pl/aktualnosci/jak-rozwoj-technologiczny-zmienia-biznes/).

Organizations also face the challenge of ensuring an adequate level of security for their resources. The expectations of society, customers, and business partners are increasing, creating a growing gap between the actual state of security and what is perceived as necessary. The main causes of this gap in the context of organizational security are:

- Rapid technological development,
- Complexity of IT infrastructure,
- Shortage of qualified personnel,
- Evolving cyber threats,
- Low security awareness among employees,
- Outdated regulations and standards.

The safety of an organization is a complex function, the value of which is conditioned by the level of risk. One of the fundamental conditions for achieving the organization's goals is to ensure the safety of its operations (Szwarc and Zaskórski, 2012). Technology is developing at a dizzying pace, introducing new products, services, and solutions. Organizations are trying to keep up with these changes to remain competitive.

However, every new technology brings new threats and vulnerabilities that require immediate response. Research on the relationships between technologies and organizations can refer to two distinct issues: the organization as a user of technology or the organization as a provider of technological solutions (Klincewicz,

2016). Maintaining an adequate level of security in the face of such dynamic changes is a huge challenge.

Another element determining the safety of the organization is IT infrastructure, particularly virtualization. The systematic popularization of virtualization technologies is inevitable, especially since users currently have a considerable choice of various solutions.

Virtualization is a technique whose potential advantages and possibilities are now widely recognized. In large data centres, server and storage virtualization is standard. The goal of virtualization is to optimize the IT environment and increase the efficiency of existing components of IT infrastructure. It allows for the integration of many independently operating IT systems, helps reduce the operating costs of the infrastructure, and ensures even utilization of its resources. Thanks to virtualization, the IT environment is better prepared for the constant changes that arise from the ongoing need to adapt to rapidly changing conditions (Rot and Chrobak, 2019).

IT infrastructure serves as the foundation on which the functioning of modern organizations is built. Without appropriate IT infrastructure, managing processes—particularly security—and optimizing resources becomes significantly more difficult, and in some cases, virtually impossible.
(https://www.engave.pl/blog/infrastruktura-it-fundament-funkcjonowania-przedsiebiorstw).

Another factor is the shortage of skilled personnel. Human resources are the most important asset of any organization (Ciekanowski, 2014). The lack of qualified security specialists is one of the main problems faced by organizations. The growing demand for experts in this field exceeds the supply, resulting in difficulties in hiring and retaining appropriate human resources. Without the right experts, organizations struggle to implement and maintain effective security strategies. An organization can develop only through factors directly conditioning its development (Ciekanowski *et al.*, 2023).

Organizations also need to constantly update their security measures to keep up with evolving threats such as ransomware, phishing, DDoS attacks, or advanced persistent threats (APTs). Dynamically changing threats require flexible and proactive defensive strategies. Practically every cyber threat is aimed at one of three goals:

- financial gain;
- disrupting the organization's operations;
- or espionage (Tuz, 2023).

As the use of new technologies increases, so does the risk of cyber attacks. Cyber attacks can have serious consequences for organizations. To minimize the risk of cyber attacks, organizations must implement appropriate solutions in the field of cybersecurity management (Ciekanowski *et al.*, 2024).

The human factor remains one of the weakest links in an organization's security. Lack of awareness and proper employee education in security leads to mistakes that can create serious security vulnerabilities. Even the best-designed security systems can be breached by unintentional employee actions. This applies to both IT competencies and threats generated by social engineering techniques (Nowicka, 2023).

Employees who are well-versed in cybersecurity principles play a key role in preventing data security incidents. Their daily habits and vigilance can significantly reduce the risk of breaches (https://szkoleniawec.pl/cyberbezpieczenstwo-w-pracy-jak-pracownicy-tworza-fundament-bezpiecznej-przyszlosci-organizacji/).

Legal regulations and industry standards often fail to keep pace with the rapid development of technology and the changing threat landscape. Organizations must operate within the existing regulations, which may be outdated and not cover new technologies and threats. This makes effective security and compliance management more difficult. The document defining the organization's security policy should contain:

- A mechanism enabling information sharing,
- A management intention statement confirming the goals and principles of information security in relation to business strategies and requirements,
- A structure for setting security objectives, including a framework for risk assessment and management,
- A brief explanation of the security policy, principles, standards, and compliance requirements that are particularly relevant to the organization.

Definitions of general and specific responsibilities regarding information security management, including reporting incidents related to information security (Bajorek, 2016).

Legal regulations broadly address issues related to ensuring the security of the operation of digital technology platforms (Bartczak and Bodych-Biernacka, 2021).

Managing security in an organization requires an integrated approach that encompasses technology, processes, and organizational culture. An effective security strategy should integrate all these elements to create a cohesive and resilient system for protecting the organization’s resources. This is an ongoing process that requires commitment at all organizational levels.

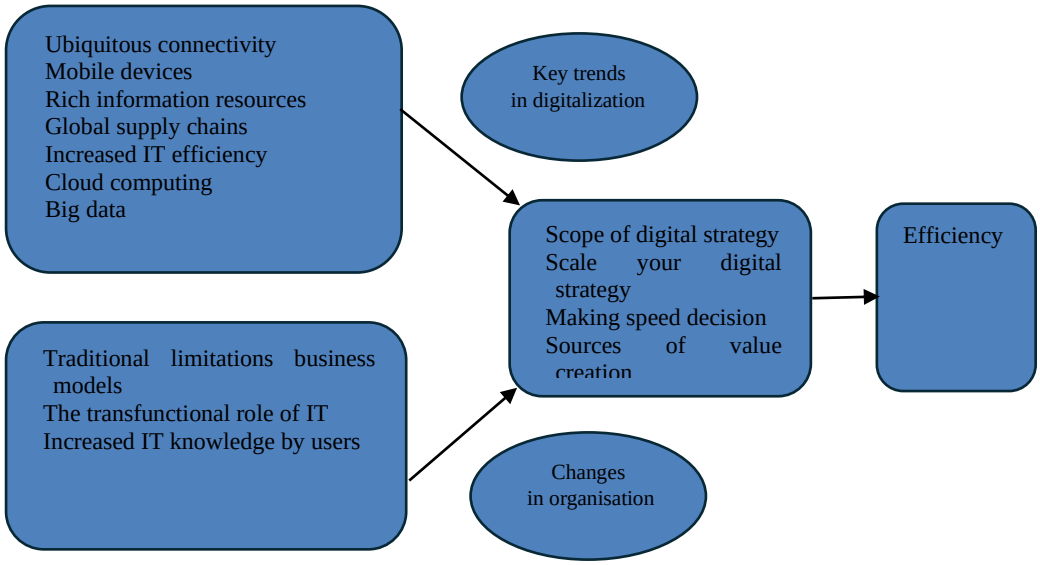
3. Organizational Management in Times of Digitization

The virtual world enables the processing and storage of an indefinite amount of information, which becomes the driving force in all areas of life, including the economic sphere and management of organizations (Stępień, 2017).

Managing an organization in the era of digital transformation is a complex task that requires a well-thought-out strategy and a flexible approach. Digital transformation is not just the implementation of new technologies, but primarily a change in organizational culture, processes, and mindset.

A key element is creating a coherent digital vision that will serve as the foundation for all activities within the organization. This vision should be closely linked to business goals and take into account the needs of both customers and employees. Organizational leaders must be engaged in the transformation process, setting an example for others and promoting an innovative approach to work. Below, the diagram presents the key elements that guide thinking towards a digital strategy and are helpful in outlining a new generation of strategies.

Figure 1. *Key elements shaping the organization's digital strategy*



Source: *Bharadwaj et al., 2013.*

Another important aspect is understanding the role of data in modern business. Organizations must learn to effectively collect, analyse, and utilize data for decision-making. This requires not only investment in appropriate analytical tools but also the development of analytical skills among employees. Data can fundamentally take three forms:

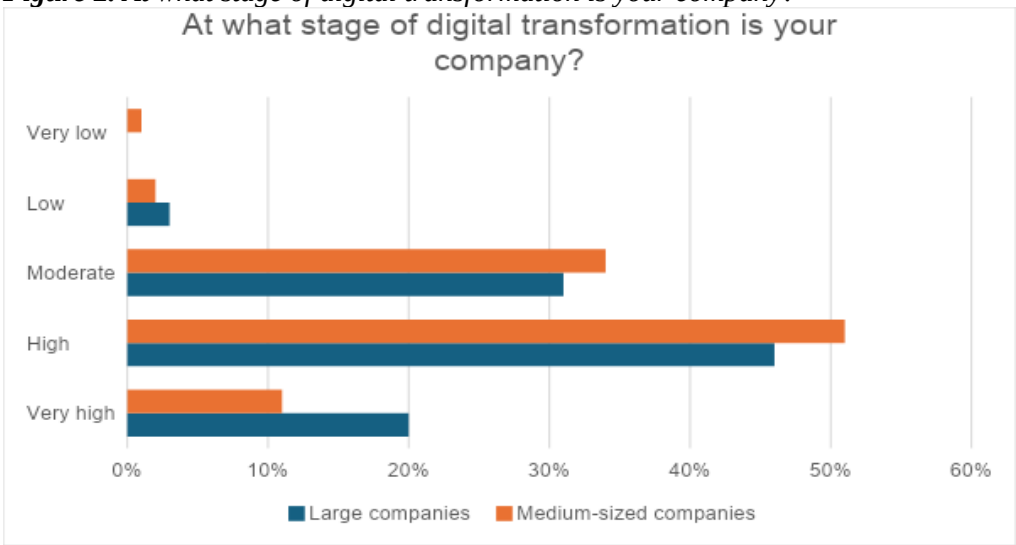
- Generating costs – for example, through the obligation to meet legal and regulatory requirements, which includes securing, deleting, or informing about them;
- Generating profits – besides the fact that they also incur costs, they can increase the organization's revenue, mainly in the area of advanced analytics, which can be "provided" both to the customer and to the organization itself;
- Being neutral – often, these are non-personal data of low value that, for various reasons, still "remain with us" – although they can also generate costs (https://bank.pl/kilka-slow-o-kulturze-danych-w-organizacji-czyli-o-strategii-zarzadzania-danymi-bez-sztucznej-inteligencji/).

Data can provide valuable insights into customer behaviour, operational efficiency, and potential areas for growth.

Digital transformation also involves the need to rethink and optimize business processes. Automating routine tasks, implementing business process management (BPM) systems, and utilizing artificial intelligence and machine learning can significantly enhance the organization's efficiency. However, it is important that these changes are introduced gradually and thoughtfully, taking into account the needs and concerns of employees.

Below, Figure 2 presents the results of a study conducted by EY, which analysed how, after years of intensive efforts in the area of digital transformation, the current approach of Polish enterprises to this process looks.

Figure 2. *At what stage of digital transformation is your company?*

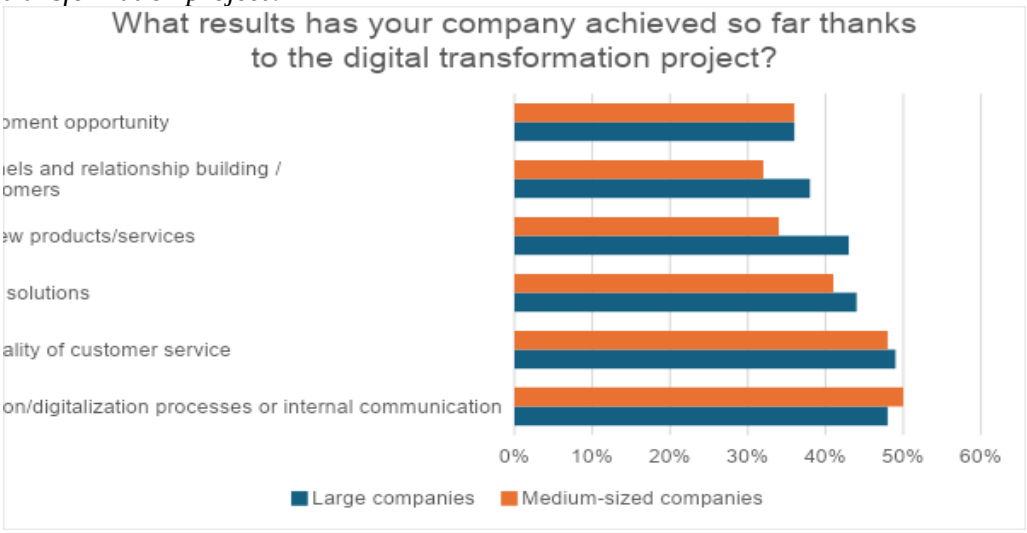


Source: *https://www.ey.com/pl_pl/raporty-analizy.*

The above data indicates that as many as 64% of the surveyed companies assess their advancement in the digital transformation process as high or very high. Particularly interesting is the disparity between large and medium-sized enterprises regarding the level of advancement achieved—one in five large companies declares that they are at a very high stage of transformation, while in the segment of medium-sized companies, only 11% make such a declaration (https://www.ey.com/pl_pl/raporty-analizy).

Digital transformation requires flexibility and a willingness to continuously learn. Technology is evolving at a dizzying pace, so organizations must be ready to adapt and continually improve their processes and strategies. Introducing a culture of innovation, supporting creativity, and being open to new ideas are key elements of success in the digital age. Below are data regarding the results achieved through the digital transformation project, also from the EY study.

Figure 3*. What results has your company achieved so far thanks to the digital transformation project?*



Source: *https://www.ey.com/pl_pl/raporty-analizy.*

As indicated by the above analysis, the effects of the digital transformation process in Polish companies are beneficial. The analysis shows that the key benefits are the automation and digitization of internal processes or communication (49%), which allows for increased work efficiency, reduction of operational costs, and elimination of manual errors, as well as improvement in customer service (48%).

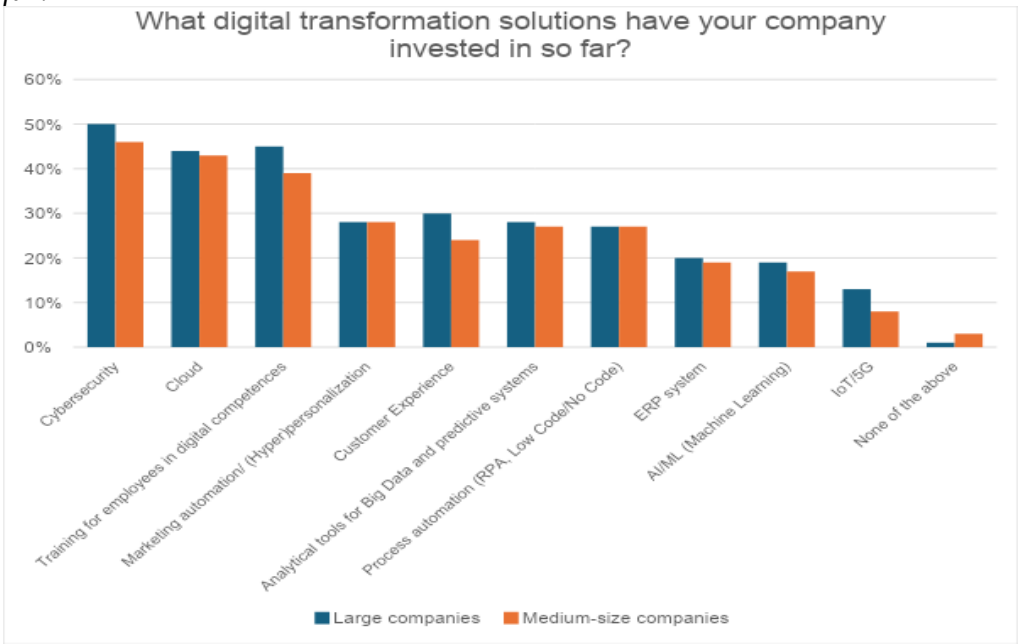
This is achieved through the implementation of advanced CRM systems and the use of chatbots and AI for handling inquiries, contributing to faster and more personalized service. The development of e-commerce, digital platforms, and social

media as channels for communication and sales is essential for maintaining competitiveness and adapting to changing consumer expectations (https://www.ey.com/pl_pl/raporty-analizy).

Technological changes also bring challenges related to cybersecurity. Organizations must invest in appropriate measures to protect data and IT systems to safeguard against cyber attacks. It is also important to train employees in digital security to raise their awareness and ability to respond to potential threats.

The factors mentioned above are elements of modern flexible organizations, meaning those that are ready to adapt efficiently and adequately to the challenges of both the internal and external environments of the organization (Ciekanowski, 2023). The chart below shows what solutions have been invested in so far within the framework of digital transformation in the surveyed companies.

Figure 4. *What digital transformation solutions have your company invested in so far?*



Source: *https://www.ey.com/pl_pl/raporty-analizy.*

The high priority of cybersecurity on the agenda is a direct reflection of the constantly increasing threat of cyberattacks. In the face of the evolving creativity of criminals and the enormous risk associated with a potential attack, this demonstrates that without appropriate cybersecurity measures, no digital initiative can be fully effective or secure (https://www.ey.com/pl_pl/raporty-analizy).

In some organizations, activity in the area of security is a fragmented and poorly organized protective effort that does not guarantee adequate results and often boils down to merely addressing the consequences of hardware and software failures (Rot, 2011).

In the process of digital transformation, one cannot forget about the customers. Modern technologies enable a better understanding of their needs and expectations, allowing for the adaptation of products and services to their requirements. Personalization, quick access to information, and convenient and intuitive user interfaces are becoming key elements in building positive customer experiences.

Managing an organization in the era of digital transformation is a complex process that requires a strategic approach, investment in technology and skills, optimization of processes, and a focus on customer needs and security. It is a challenge, but at the same time, a tremendous opportunity for growth and increased competitiveness in the market.

4. Conclusions

Digital transformation introduces a series of changes that revolutionize the way organizations operate and their security. The increased use of digital technologies brings enormous benefits but also presents new challenges in terms of security.

Modern organizations must not only secure their IT systems but also adapt their approach to security management to the dynamically changing digital environment. With technological advancements, new types of threats and attacks emerge. Cybercriminals are becoming increasingly sophisticated, which requires the use of advanced tools and defence methods.

Information systems are becoming more integrated, increasing the risk of security vulnerabilities. This necessitates a holistic approach to security management that encompasses both technologies and security procedures and policies. Organizations must not only implement appropriate protective measures but also regularly monitor and audit their systems to ensure compliance.

Training employees and building a culture of security within the organization are essential. Employees often represent the weakest link in the security system, so their education about threats and safe practices is crucial.

Organizations should adopt a proactive approach to security management, focusing on prevention and early detection of threats rather than merely reacting after an incident occurs. Thus, the research hypothesis has been confirmed.

Security must be tailored to the specific characteristics of the organization and its digital environment. Flexible and scalable security strategies allow for quicker responses to changing conditions.

References:

Bajorek, J. 2016. Ochrona i bezpieczeństwo danych osobowych w organizacji. De Securitate et Defensione. O Bezpieczeństwie i Obronności, nr 1/2016.

Bartczak, K., Bodych-Biernacka, M. 2021. Rodzaje cyberzagrożeń i prawne sposoby im przeciwdziałania w kontekście stosowania cyfrowych platform technologicznych w Polsce i UE. Przegląd Organizacji, Nr 3(974).

Bharadwaj, A., El Sawy, O.A., Pavlou, P.A., Venkatraman, N. 2013. Digital Business Strategy: Toward a Next Generation of Insights. MIS Quarterly, No. 37(2)/2013.

Ciekanowski, Z. 2023. Wsparcie informacyjne systemu zarządzania kryzysowego. MANS, Warszawa.

Ciekanowski, Z. 2014. Kapitał ludzki najistotniejszym elementem w organizacji. Seria: Administracja i Zarządzanie 28, nr. 101.

Ciekanowski, Z., Nowicka, J., Żurawski, S., Mikosik, P. 2023. Human Resources in Organizational Security Management. European Research Studies Journal, Volume XXVI, Issue 4.

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.

Cyberbezpieczeństwo w pracy: jak pracownicy tworzą fundament bezpiecznej przyszłości organizacji. https://szkoleniawec.pl/cyberbezpieczenstwo-w-pracy-jak-pracownicy-tworza-fundament-bezpiecznej-przyszlosci-organizacji/.

Infrastruktura IT: fundament funkcjonowania przedsiębiorstw. https://www.engave.pl/blog/infrastruktura-it-fundament-funkcjonowania-przedsiebiorstw.

Jak rozwój technologiczny zmienia biznes? https://www.it.integro.pl/aktualnosci/jak-rozwoj-technologiczny-zmienia-biznes/.

Kilka słów o kulturze danych w organizacji, czyli o strategii zarządzania danymi (bez sztucznej inteligencji). https://bank.pl/kilka-slow-o-kulturze-danych-w-organizacji-czyli-o-strategii-zarzadzania-danymi-bez-sztucznej-inteligencji/.

Klincewicz, K. 2016. Zarządzanie technologiami – perspektywa organizacji-użytkownika. In: Klincewicz, K. (red.), Zarządzanie, organizacje i organizowanie – przegląd perspektyw teoretycznych, Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warszawa.

Nowicka, J. 2023. Kompetencje komunikacyjne i społeczne w obszarze bezpieczeństwa. Po drugie – GRUPA. Akademia Sztuki Wojennej, Warszawa, t. 2.

Raport: Czy Twój biznes zanurzył się w cyfrowej transformacji, czy tylko powierzchownie dotknął jej możliwości? Transformacja Cyfrowa 2024, EY. https://www.ey.com/pl_pl/raporty-analizy.

Rot, A. 2011. Zastosowanie modeli dojrzałości w zarzadzaniu ryzykiem na potrzeby bezpieczeństwa systemów informatycznych w organizacji. Informatyka Ekonomiczna, nr. 19.

Rot, A., Chrobak, P. 2019. Optymalizacja wykorzystania zasobów infrastruktury IT jako element budowy przewagi konkurencyjnej organizacji. Roczniki Kolegium Analiz Ekonomicznych, z. 54.

Stępień, A. 2017. Bezpieczeństwo w erze cyfryzacji. Przedsiębiorczość i Zarządzanie, nr 5.2.

Szwarc, K., Zaskórski, P. 2012. Identyfikacja zagrożeń dla ciągłości działania organizacji. Studia Bezpieczeństwa Narodowego, nr 1, vol. 3.

Tuz, M. 2023. Wpływ cyberzagrożeń na funkcjonowanie organizacji. Przegląd Policyjny, nr 3.

Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E., Thalassinos, E. (Eds.). 2023. Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy. Emerald Publishing Limited.

Velinov, E., Kadłubek, M., Thalassinos, E., Grima, S., Maditinos, D. 2023. Digital Transformation and Data Governance: Top Management Teams Perspectives. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (Vol. 111, pp. 147-158). Emerald Publishing Limited.

Ziarko, J. 2019. Podejście systemowe w badaniach bezpieczeństwa organizacji. Bezpieczeństwo. Teoria i Praktyka, nr. 4.