Politechnika Częstochowska
Wydział Zarządzania

Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie
Research Reviews of Czestochowa University of Technology. Management

No. 63 (2026), pp. 34-44, ISSN: 2083-1560, e-ISSN: 3071-9259
DOI: 10.17512/znpcz.2026.3.03, http://znz.pcz.pl

Received: 26.06.2026; Revised: 08.08.2026;
Accepted: 11.08.2026; Published: 30.09.2026.

DEFINING CYBERSECURITY MANAGEMENT

Konrad Głębocki[1*]

[1] Czestochowa University of Technology, Management Faculty, Poland

Abstract: Cybersecurity has become one of the most important topics in both academic research and the practice of public and private organizations. Relatively little attention, however, has been devoted to the management of cybersecurity itself. Central to this article is a literature review encompassing 30 scholarly publications published over the past decade. The review, conducted from the perspective of cybersecurity management, identified the following areas that are directly or indirectly related to this subject: cyber incidents and protection tools, cybersecurity, and cybersecurity management itself. Based on the literature review, the author derived 17 concise statements that serve as a foundation for defining cybersecurity management. Following an analysis of these statements, the author formulated a proposed definition of cybersecurity management.

Keywords: cyberattacks, cybersecurity, cybersecurity management

JEL Classification: M15, O33

Introduction

A certain paradox can be observed: while an increasingly digitalized public administration generates growing financial, organizational, and communicative benefits, the advancement of technology simultaneously exposes organizations to more numerous and increasingly sophisticated cyberattacks. As a result, public administration is becoming progressively more vulnerable (Oleksiewicz, 2020). The society's dependence on information and communication technologies continues to increase, while these technologies themselves are characterized by complex interdependencies among various actors and networks of organizations (Leppänen

[1] Konrad Głębocki, Associate Professor, konrad.glebocki@pcz.pl,
https://orcid.org/0000-0001-7241-7970
* Corresponding author: Konrad Głębocki, konrad.glebocki@pcz.pl

& Kankaanranta, 2020). Consequently, the need to ensure cybersecurity is becoming more and more pressing. Given the nature of cybersecurity, developing cybersecurity capabilities cannot be the responsibility of a single organization; rather, it requires the involvement of all types of actors operating in cyberspace, including both private entities and public organizations (Bederna et al., 2021).

Methodology

The aim of this article is to propose a definition of cybersecurity management. The proposed definition was inductively derived from a literature review. The goal of the literature review was to find and analyze sources useful in the construction of the definition of cybersecurity management. Next, these sources were classified into areas indirectly and directly related to cybersecurity management to achieve clarity and help in the construction of the definition. The keywords to be used in search engines of Taylor and Francis, Google Scholar, EBSCO and Elsevier were 'cybersecurity management' and 'cybersecurity management definition'. The selection criteria were: novelty – because of the rapid pace of change in the field (meaning: picking up most sources from the last ten years, not older than 2015) and a potential contribution to the design of the definition of cybersecurity management (potential contribution arbitrarily decided by the author).

The review encompassed more than 30 scholarly publications published between 2015 and 2025, the majority of which were international studies, supplemented by several Polish publications. The article draws upon research concerning both public and private sector organizations. The literature review identified several areas related to cybersecurity management, including cyber incidents and protective measures, cybersecurity, and cybersecurity management itself.

Following an analysis of the reviewed literature, the author formulated 17 concise statements that serve as a foundation for defining cybersecurity management. The synthesis of the various elements contained within these statements enabled the development of a proposed definition of cybersecurity management that is grounded in the broader understanding of management as a paradigm. Based on the analysis of these statements, the author subsequently formulated a proposed definition of cybersecurity management. The recommended structure of the article includes the following parts: Introduction; Methodology; Literature Review; Results – Defining cybersecurity management and discussion; Conclusion.

Cyber incidents and protection tools

Cyber incidents, understood as disruptions in the routine functioning and operations of digital technologies, have gained exceptional importance in state policy and at the international level. Cyberattacks are becoming increasingly targeted and, in many cases, carry political and strategic significance (Cavelty & Wenger, 2020). The protection of public institutions, private entities, and society against cyberattacks is one of the most important tasks of the state, which should meet the needs of society to the greatest possible extent (Karpiuk, 2021).

Cybersecurity must also address internal threats caused intentionally or unintentionally by employees of public organizations. A culture of cybersecurity can help in detecting these threats (Georgiadou et al., 2022). The increasing complexity and expanding scope of cyberattacks pose a growing threat to the functioning of public entities. There is an urgent need for effective cybersecurity management and to combat cyberattacks in a holistic and comprehensive manner, involving all functional areas (Dominguez-Dorado et al., 2023). Moreover, the significantly rising level of cyberattacks makes it almost certain that any organization can become a victim of a cyberattack at any time (Islam et al., 2025).

The term "cybersecurity incident management" refers to three phases: identification, management, and mitigation of the effects of cyber incidents (Jones et al., 2025). It is difficult to agree with such an interpretation if management were understood as only one of the components of cybersecurity incident management.

According to the Ponemon Institute, the most common cyberattacks include ransomware, DDoS, viruses and bots, DNS attacks, and phishing (Kshetri, 2021). The listed cyberattacks consist of:

1. Attacks involving the blocking of an organization's data for ransom (ransomware).
2. A Distributed Denial-of-Service (DDoS) attack is a malicious attempt to disrupt the normal functioning of a server, service, or network by overwhelming it with a massive amount of internet traffic coming from multiple compromised systems (a so-called botnet). Such attacks render online services unavailable to legitimate users (Douligeris & Mitrokotsa, 2004), causing downtime, financial losses, and reputational damage.
3. Viruses and bots.
4. DNS-based attacks (Domain Name System) target the Domain Name System (DNS), which translates human-readable domain names into IP addresses. Since DNS is essential for nearly all internet activity, its disruption can paralyze an organization's digital operations (Nuiaa et al., 2022).
5. Phishing primarily involves email-based hacking, where the recipient clicks a link included in a message from the sender and is redirected to a hacker-controlled website that may resemble an official bank website. Entering data on such a site allows the attacker to obtain information that can be used to cause harm (Bhavsar et al., 2018).

Tools developed and implemented by public entities to counter threats in cyberspace can take various forms, from education and training, through technologies and related standards, to new legal frameworks and strategic actions (Creese et al., 2021). In some cases, public organizations are able to develop cybersecurity tools that also benefit non-public entities such as small and medium-sized enterprises (Lee & Park, 2015).

The costs of remedying damage resulting from cyberattacks are becoming increasingly high (Cavelty & Wenger, 2020). Developing tools to prevent cyberattacks may be less expensive than repairing the resulting damage. The largest expenditures related to cybersecurity protection tools are associated with appropriate technologies. Smaller costs concern the development of corporate security policies and employee training (Fuksiewicz, 2023).

DOI: 10.17512/znpcz.2026.3.03

As to the number of cyber incidents in Poland handled by the state unit CERT, which is the team fighting cyber incidents, the table below shows the numbers in the breakdown by years 2018-2025.

Table 1. Breakdown of the number of incidents handled by CERT Polska by years 2018-2025

Year	Number of incidents
2025	260 783
2024	103 449
2023	80 267
2022	39 683
2021	29 483
2020	10 420
2019	6 484
2018	3 739

Source: Annual Activity Report (CERT Polska, 2025)

Following the results shown in the table above, one can state that the number of incidents handled by CERT is growing every year. Sometimes, the numbers year to year are doubled (the year 2022 to 2023; the year 2024 to 2025) or even tripled (the year 2020 to 2021).

Notion of cybersecurity

The concept of cybersecurity emerges from the revolution in access to information, which in turn results from the recent information technology revolution. In the literature, there is no single universally accepted concept of information (Banasiński, 2018), nor is there a single definition of cybersecurity. This applies to both the meaning and the scope of definitions; sometimes mutually contradictory terms are used. Moreover, it is noted that most definitions are related to public organizations (Schatz et al., 2017).

The simplest definition of cybersecurity states that it is the security of information in cyberspace. Another, broader definition describes cybersecurity as the organization and set of resources, processes, and structures used to protect cyberspace and cyberspace-based systems from events that cause discrepancies between formal (de jure) and actual (de facto) property rights (Craigen et al., 2014).

Based on broader research into existing definitions, an even more comprehensive definition has been developed: An approach and activities related to security risk management processes applied by both organizations and states, associated with the confidentiality, integrity, and availability of data and resources used in cyberspace. The concept includes guidelines, policies, and sets of safeguards, technologies, tools, and training aimed at ensuring the best possible protection of the cyber environment and its users (Schatz et al., 2017).

In the document "Cybersecurity Doctrine of the Republic of Poland," a distinction is made between the concepts of "Cybersecurity of the Republic of Poland" and "Security in the Cyberspace of the Republic of Poland." The former is defined as a broader concept, encompassing the process of ensuring the safe functioning in cyberspace of the state and various public and private entities, as well as the teleinformation systems and information resources at their disposal. The latter, in turn, includes a set of activities of various nature (organizational-legal, technical, physical, and educational) aimed at the uninterrupted functioning of the cyberspace of the Republic of Poland (Mąkosa, 2019).

According to the International Telecommunication Union (ITU), cybersecurity is a set of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, insurance, and technologies that can be used to protect the cyber environment, organizations, and users' assets. The organization and users' assets include connected computers, personnel, infrastructure, applications, services, telecommunications systems, and all transmitted and/or stored information in the cyber environment (Kshetri, 2021).

Cybersecurity management

The concept of 'cybersecurity management' in the literature is not primarily emphasized; instead, the narrower concept of 'cybersecurity risk management' is highlighted. It is considered that the latter concept is critical for any organization, so that decisions are based on an appropriate scope of information in order to manage risks before they materialize. Cybersecurity risk management is contextual in nature and is based on the specific context of an organization (Islam et al., 2025).

Another term that frequently appears in the context of cybersecurity management is trust management (TM), which encompasses strategies aimed at ensuring the security and privacy of digital systems. By implementing these strategies, organizations build and maintain trust in their digital environments, mitigating cybersecurity risks and ensuring, among other things, the integrity of sensitive information (Pigola & de Souza Meirelles, 2024).

In connection with the above terms related to management, which narrow the concept to a specific field, the term Cybersecurity Management System has emerged. This term encompasses various elements of cybersecurity management, including asset management, incident management, and change management (Negi et al., 2025). The aforementioned risk management and trust management in cybersecurity are also part of a cybersecurity management system. Additional qualifiers are also used in relation to the concept of the system itself, as in the case of the New Resilient Cybersecurity Management System for Connected and Automated Vehicles (Guang et al., 2025).

Cybersecurity management can be examined from various perspectives, for example, in relation to efforts aimed at improving cybersecurity among municipalities. It has been demonstrated that the larger the local government at the basic level, the greater its engagement in cybersecurity activities. Moreover, a moderately positive

effect has been found regarding the amount of employee time devoted to cybersecurity. The research was conducted on municipalities in Sweden (Karlsson et al., 2025).

In Poland, there are numerous legal acts concerning the obligation to implement information security management (Lisiak-Felicka & Pytko, 2017). In survey-based research conducted among municipalities in the Łódź Voivodeship, issues such as the implementation of an information security management system were examined. Out of 177 municipal offices, only 44 responded, of which 31 had implemented an information security management system (Lisiak-Felicka & Pytko, 2017). It can be assumed that many of the offices that did not respond to the survey simply did not have an information security management system in place.

Strategic cybersecurity leadership involves identifying and defining goals based on the protection of the digital operational environment. It also entails coordinating activities and managing major disruptions (Lehto & Limnell, 2021).

Cybersecurity management is significantly influenced by both economic and technological factors. Moreover, cybersecurity management acts as a key mediator in the relationship between these factors and firm performance (Zaidan & Massoudi, 2025).

There are also bibliometric studies concerning, among other things, cybersecurity in management. However, in detail, they focus primarily on risk management, which is treated in the research with less attention than threat detection and protection against threats (Al-Shattarat et al., 2025).

A broad definition of cybersecurity management includes not only management itself in the strict sense, but also policies and investment in cybersecurity protection (Norris et al., 2022).

Defining cybersecurity management and discussion

In the academic literature, many definitions of management can be found. Similarly, in the literature on cybersecurity, cybersecurity management is understood in various ways. A proposed paradigm for defining cybersecurity management is the definition of management itself: "Management consists in the use of various resources, including financial, material, and human resources, to achieve intended goals."

Below are 17 concise statements derived from the literature review, which will serve as a basis for formulating a definition, taking the indicated paradigm into account.

1. Cyber incidents are disruptions in the operations of digital technologies (Cavelty & Wenger 2020).
2. Defending an organization against cyberattacks is one of its most important tasks (Karpiuk, 2021).
3. Cybersecurity threats may originate from within an organization (Georgiadou et al., 2022).
4. Countering cyberattacks must be holistic in nature (Dominguez-Dorado et al., 2023).
5. The most common cyberattacks include ransomware, DDoS attacks, viruses and bots, DNS attacks, and phishing (Kshetri, 2021; Douligeris & Mitrokotsa, 2004; Nuiaa et al., 2022; Bhavsar et al., 2018).

6. Tools for protection against cyberattacks include appropriate technologies, corporate security policies, and employee training (Creese et al., 2021).
7. Cybersecurity is the organization and set of resources, processes, and structures used to protect cyberspace and cyberspace-based systems from events that cause discrepancies between formal (de jure) and actual (de facto) property rights (Craigen et al., 2014).
8. Cybersecurity is an approach and set of activities related to risk management processes applied by organizations and states, connected with the confidentiality, integrity, and availability of data and resources used in cyberspace (Schatz et al., 2017).
9. A cybersecurity doctrine is a process concerning the secure functioning of various entities in cyberspace, as well as the tele information systems and information resources at their disposal (Mąkosa, 2019).
10. Cybersecurity of the Republic of Poland is a set of organizational, legal, technical, physical, and educational measures aimed at ensuring the uninterrupted functioning of the cyberspace of the Republic of Poland (Mąkosa, 2019).
11. Cybersecurity is a set of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, insurance, and technologies that can be used to protect the cyber environment, organizations, and user resources (Kshetri, 2021).
12. A Cybersecurity Management System includes asset management, incident management, change management, risk management, and trust management (Islam et al., 2025; Pigola & de Souza Meirelles, 2024; Negi et al., 2025).
13. A moderate positive effect on cybersecurity is exerted by a greater amount of employee time devoted to cybersecurity (Karlsson et al., 2025).
14. Few municipalities in the Łódź Voivodeship declare the implementation of an information security management system (Lisiak-Felicka & Pytko, 2017).
15. Strategic cybersecurity leadership involves identifying and defining goals based on the protection of the digital operational environment, coordinating activities, and managing major disruptions (Lehto & Limnell, 2021).
16. Cybersecurity management is significantly influenced by both economic and technological factors (Zaidan & Massoudi, 2025).
17. Cybersecurity management includes, in addition to management in the strict sense, also policies and investment in cybersecurity (Norris et al., 2022).

Analysis of the above statements makes it possible to formulate the following proposed definition (in brackets, the numbers refer to the numbering of the statements above, thereby indicating which elements of the definition correspond to which specified statements):

"Cybersecurity management includes strategic leadership (15) in among others risk (8), change, and trust management (12), and is about the appropriate use of technological (6, 10, 16), economic (16, 17), organizational, and human (6, 10, 13) resources of an organization (7) in order to create a secure cyber environment (11) and protect the organization (9) against cyber incidents (1, 2, 4, 5) originating both internally (3) and externally, including those concerning information protection (9, 14)."

This definition does not refer to the term "Cybersecurity Management System." The term "system" would imply a set of ordered and interrelated elements. At this stage, it would be difficult to formulate a definition meeting these criteria.

The final form of the proposed definition, without numerical references to the statements derived from the literature, is as follows:

"Cybersecurity management includes strategic leadership in among others risk, change, and trust management, and is about the appropriate use of technological, economic, organizational, and human resources of an organization in order to create a secure cyber environment and protect the organization against cyber incidents originating both internally and externally, including those concerning information protection."

It is hard to refer to the above definition to the definitions formulated so far in the literature because scholars were defining, first of all, cybersecurity. Cybersecurity, as a wider term, replaced the term information security (von Solms & von Solms, 2018). The definition proposed by the author is wider than both information security and cybersecurity. The author did not find even one clear definition of cybersecurity management in the up-to-date literature. Sources that have cybersecurity management in the title are very scarce, and even these sources do not present a clear definition (Yereshko et al., 2026), Pigola & da Costa, 2025). It remains in contrast to many sources that are about cybersecurity risk management (Khalifa & Taha, 2026; Siyaya et al., 2025; Lakhno et al., 2026).

Nine definitions of cybersecurity recalled by Schiliro predominantly describe cybersecurity as a process or a practice, which seems to be a good step in the direction of a definition of cybersecurity management (Schiliro, 2023). But none of these definitions is close in its construction to the definition of cybersecurity management in the paper.

Conclusions

The aim of the article was to formulate a proposed definition of cybersecurity management. This definition was derived inductively based on a literature review. From this review, several areas related to cybersecurity management emerged: cyber incidents and protection tools, cybersecurity, and cybersecurity management itself. After analyzing the literature review, the author identified 17 concise statements as an initial step toward defining cybersecurity management. The synthesis of various elements of these 17 statements in the literature enabled the formulation of a proposed definition of cybersecurity management, referring to the definition of management itself as a paradigm. After analyzing these statements, the author formulated a proposed definition of cybersecurity management.

The proposal is as follows: "Cybersecurity management includes strategic leadership in, among others, risk, change, and trust management, and is about the appropriate use of technological, economic, organizational, and human resources of an organization in order to create a secure cyber environment and protect the organization against cyber incidents originating both internally and externally, including those concerning information protection".

References

Al-Shattarat, W., Benameur, K., Mostafa, M. M., Hassanein, A., & Hamed, R. S. (2025). A decade of cybersecurity research in business, management, and accounting: Bibliometric analyses and future research directions. *Cogent Business & Management*, *12*(1), 1-26. https://doi.org/10.1080/23311975.2025.2544230

Banasiński, C. (2018). Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni. In C. Banasiński (Red.), *Cyberbezpieczeństwo. Zarys wykładu* (pp. 21-65). Wolters Kluwer Polska.

Bederna, Z., Rajnai, Z., & Szadeczky, T. (2021). Business strategy analysis of cybersecurity incidents. *Revista Academiei Forţelor Terestre*, *26*(2), 139-149. https://doi.org/10.2478/raft-2021-0020

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. *International Journal of Computer Applications*, *182*(33), 27-29. https://doi.org/10.5120/ijca2018918286

Cavelty, M. D., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32. https://doi.org/10.1080/13523260.2019.1678855

CERT Polska. (2026). *Raport roczny 2025 z działalności CERT Polska – Krajobraz bezpieczeństwa polskiego Internetu*. Państwowy Instytut Badawczy NASK.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13-21. https://doi.org/10.22215/timreview/835

Creese, S., Dutton, W. H., Esteve-González, P., & Shillair, R. (2021). Cybersecurity capacity-building: Cross-national benefits and international divides. *Journal of Cyber Policy*, *6*(2), 214-235. https://doi.org/10.1080/23738871.2021.1979617

Dominguez-Dorado, M., Rodríguez-Pérez, J., Carmona-Murillo, J., Cortés-Polo, D., & Calle-Cancho, J. (2023). Boosting holistic cybersecurity awareness with outsourced wide-scope CyberSOC: A generalization from a Spanish public organization study. *Information*, *14*, Article 586. https://doi.org/10.3390/info14110586

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Networks*, *44*(5), 643-666. https://doi.org/10.1016/j.comnet.2003.10.003

Fuksiewicz, M. (2023). Rodzaje i cechy charakterystyczne cyberataków oraz zarys działań w obszarze cyberbezpieczeństwa. *Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu*, *102*(3), 51-63. https://doi.org/10.58683/dnswsb.615

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Detecting insider threat via a cyber-security culture framework. *Journal of Computer Information Systems*, *62*(4), 706-716. https://doi.org/10.1080/08874417.2021.1903367

Guang, H., He, J., Zheng, B., Gong, W., Shi, J., Wu, H., Cao, J., Yang, S., & Karimi, H. R. (2025). Perspective: A novel resilient cybersecurity management system for connected and automated vehicles. *Automotive Innovation*, *8*, 335-367. https://doi.org/10.1007/s42154-025-00355-x

Islam, S., Basheer, N., Papastergiou, S., Ciampi, M., & Silvestri, S. (2025). Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. *Journal of Reliable Intelligent Environments*, *11*, Article 12. https://doi.org/10.1007/s40860-025-00253-3

Jones, G., Kasimatis, D., Pitropakis, N., Macfarlane, R., & Buchanan, W. J. (2025). Analysing the role of LLMs in cybersecurity incident management. *International Journal of Information Security*, *24*, Article 228. https://doi.org/10.1007/s10207-025-01144-7

Karlsson, D., Boholm, M., & Berlin, J. (2025). Does inter-municipal collaboration strengthen cybersecurity?. *Journal of Cyber Policy*, *10*, 298-317. https://doi.org/10.1080/23738871.2026.2642608

Karpiuk, M. (2021). Organisation of the national system of cybersecurity: Selected issues. *Studia Iuridica Lublinensia*, *30*(2), 233-244. https://doi.org/10.17951/sil.2021.30.2.233-244

Khalifa, M., & Taha, A. (2026) AI-driven cybersecurity risk management in organizations: Threat intelligence, automation, and resilience. *World Research of Business Administration Journal*, *6*(1), 50-66. https://doi.org/10.56830/WRBA03202604

Kshetri, N. (2021). *Cybersecurity management: An organizational and strategic approach*. University of Toronto Press. https://doi.org/10.3138/9781487531249

Lakhno, V., Kasatkin, D., Mohylnyi, H., Desiatko, A., Zhyrova, T., Khorolska, K., & Kotenko, N. (2026). Application of cognitive and cyber modelling for cybersecurity risk management in Automated Process Control Systems. *Journal of Electronics and Telecommunications*, *72*(3), 1-9. https://doi.org/10.24425/ijet.2026.1713

Lee, Y., & Park, J. (2015). Value creation and value capture: The case of Cybershelter for information systems security in South Korea. *Journal of Information Technology Case and Application Research*, *17*, 74-92. https://doi.org/10.1080/15228053.2015.1041351

Lehto, M., & Limnell, J. (2021). Strategic leadership in cyber security: Case Finland. *Information Security Journal: A Global Perspective*, *30*(3), 139-148. https://doi.org/10.1080/19393555.2020.1813851

Leppänen, A., & Kankaanranta, T. (2020). Co-production of cybersecurity: A case of reported data system break-ins. *Police Practice and Research*, *21*(1), 78-94. https://doi.org/10.1080/15614263.2018.1525382

Lisiak-Felicka, D., & Pytko, M. (2017). Cyberbezpieczeństwo urzędów gmin w województwie łódzkim. *Przedsiębiorczość i Zarządzanie*, *18*(4), 439-451.

Mąkosa, G. (2019). Zarządzanie ryzykiem jako determinanta cyberbezpieczeństwa. *Nowoczesne Systemy Zarządzania*, *14*(3), 67-80. https://doi.org/10.37055/nsz/132731

Negi, R., Kant, V., Angelin, A., Lakshana, L. N., Singh, A., & Shukla, S. K. (2025). Augmenting analyst thinking through human-centered design to enable asset management in cybersecurity. *Cognition, Technology & Work*, *27*, 525-540. https://doi.org/10.1007/s10111-025-00812-x

Norris, D. F., Mateczun, L. K., & Forno, R. F. (2022). Managing local government cybersecurity. In D. F. Norris, L. K. Mateczun, & R. F. Forno (Eds.), *Cybersecurity and local government* (pp. 85-111). Wiley. https://doi.org/10.1002/9781119788317.ch6

Nuiaa, R., Manickam, S., & Alsaeedi, A. H. (2022). A comprehensive review of DNS-based distributed reflection denial of service (DRDoS) attacks: State-of-the-art. *International Journal on Advanced Science, Engineering and Information Technology*, *12*(6), 2452-2461. https://doi.org/10.18517/ijaseit.12.6.17280

Oleksiewicz, I. (2020). Reforma polityki cyberbezpieczeństwa Unii Europejskiej. *Teka of Political Science and International Relations*, *15*(2), 7-23. https://doi.org/10.17951/teka.2020.15.2.7-23

Pigola, A., & da Costa, P. R. (2025). Cybersecurity management: an empirical analysis of dynamic capabilities framework for enhancing cybersecurity intelligence. *Information and Computer Security*, *33*(4), 473-498. https://doi.org/10.1108/ICS-08-2024-0185

Pigola, A., & de Souza Meirelles, F. (2024). Unraveling trust management in cybersecurity: Insights from a systematic literature review. *Information Technology and Management*, *27*, 71-93. https://doi.org/10.1007/s10799-024-00438-x

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 53-74. https://doi.org/10.15394/jdfsl.2017.1476

Schiliro, F. (2023). Towards a Contemporary Definition of Cybersecurity. *arXiv preprint arXiv:2302.02274.* https://doi.org/10.48550/arXiv.2302.02274

Siyaya, M. C., Dubihlela, J., & Sibanda, M. (2025). A literature review of internal auditing involvement in cybersecurity risk management of the organization. *Journal of Contemporary Management*, *22*, Special Issue 1, 89-115. https://doi.org/10.35683/jcm24.030.293

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where?. *Information and Computer Security*, *26*(1), 2-9. https://doi.org/10.1108/ICS-04-2017-0025

Yereshko, J., Bozhinov, P., Udovychenko, I., Dobrovolskienė, N., & Tsimoshynska, O. (2026). A dual-layer hybrid security framework: analyzing digital models to enhance cybersecurity management for start-ups and SMEs. *Business Management*, *36*(1), 52-67. https://doi.org/10.58861/tae.bm.2026.1.03

Zaidan, M. N., & Massoudi, A. H. (2025). The impact of technological and economic factors on cybersecurity management and MSME performance. *International Business and Management Review*, *20*(3), 1-16. https://doi.org/10.18568/internext.v20i03.847

Authors' Contribution: Konrad Głębocki – 100%.

Acknowledgements and Financial Disclosure: There was the lack of funding used in this publication.

Conflict of Interest: There was no conflict of interest or a potential conflict of interest.

Ethics Declaration: No ethical clearance was required for the research.

AI Declaration: No AI tools were used in the creation of the paper.

DEFINIOWANIE ZARZĄDZANIA CYBERBEZPIECZEŃSTWEM

Streszczenie: Cyberbezpieczeństwo stało się jednym z najważniejszych tematów zarówno w badaniach naukowych, jak i w praktyce organizacji publicznych oraz prywatnych. Jakkolwiek stosunkowo mało uwagi poświęca się samemu zarządzaniu cyberbezpieczeństwem. Centralnym punktem artykułu jest przegląd literatury obejmujący 30 publikacji naukowych opublikowanych w ciągu ostatniej dekady. Na podstawie przeglądu, przeprowadzonego z perspektywy zarządzania cyberbezpieczeństwem, wytypowano następujące obszary, które bezpośrednio lub pośrednio dotyczą tego tematu: cyberincydenty i narzędzia ochrony, cyberbezpieczeństwo oraz samo zarządzanie cyberbezpieczeństwem. Przegląd literatury umożliwił wyprowadzenie 17 zwięzłych twierdzeń służących za fundament definiowania zarządzania cyberbezpieczeństwem. Po analizie tych stwierdzeń sformułowano zaproponowaną definicję zarządzania cyberbezpieczeństwem.

Słowa kluczowe: cyberataki, cyberbezpieczeństwo, zarządzanie cyberbezpieczeństwem

Articles published in the journal are made available under Creative Commons Attribution 4.0 International.
Certain rights reserved for the Czestochowa University of Technology.

