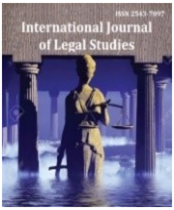

Received: 09 December 2023
Revised: 15 December 2023
Accepted: 22 December 2023
Published: 31 December 2023

CYBERSECURITY MANAGEMENT – CURRENT STATE AND DIRECTIONS OF CHANGE

ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM – STAN OBECNY ORAZ KIERUNKI ZMIAN

Mirosław Karpiuk
Prof. Dr. Hab., University of Warmia and Mazury in Olsztyn
Faculty of Law and Administration, Department of Administrative Law and Security Sciences
Obitza 1 St, 10-725 Olsztyn, Poland
ORCID: https://orcid.org/0000-0001-7012-8999
* *Corresponding author:* e-mail: miroslaw.karpiuk@uwm.edu.pl

Wojciech Pizło
Prof. Dr hab. Eng., Warsaw University of Life Sciences
Institute of Management
Nowoursynowska 166 St, 02-787 Warsaw, Poland
ORCID: https://orcid.org/0000-0002-5212-0990
* *Corresponding author:* e-mail: wojciech_pizlo@sggw.edu.pl

Krzysztof Kaczmarek
PhD, Koszalin University of Technology,
Faculty of Humanities
Eugeniusza Kwiatkowskiego 6e St, 75-343 Koszalin, Poland
ORCID: https://orcid.org/0000-0001-8519-1667
* *Corresponding author:* e-mail: puola@tlen.pl

Abstract

The objective of this paper is to analyse the threats arising from the rapid development of information and communication technologies (ICTs) without which contemporary information-based societies would not be able to function properly. The authors have advanced the thesis that most perpetrators turn to social engineering methods to carry out cyberattacks, while users of information systems are the weakest links of every cybersecurity management system. The article is also an attempt to define the notions of cybersecurity and cybersecurity management. To this end, the authors have analysed the applicable legal regulations.

ISSN 2543-7097 / E-ISSN 2544-9478

Karpiuk M., Pizło W., Kaczmarek K.,(2023). Cybersecurity Management – Current State and Directions of Change
International Journal of Legal Studies, 2(14)2023: 645 - 663
DOI 10.5604/01.3001.0054.2880

They have also explored cyberthreats to which small and medium-sized enterprises are exposed, and demonstrated opportunities for further research into the issues being discussed.

Keywords: cybersecurity management, crisis management, digital society, ICT systems, critical infrastructure

Streszczenie

Celem artykułu jest dokonanie analizy zagrożeń jakie niesie za sobą szybki rozwój technologii komunikacyjno-informacyjnych, bez których współczesne, oparte na dostępie do informacji, społeczeństwa nie są w stanie prawidłowo funkcjonować. Autorzy postawili tezę, że większość cyberataków jest dokonywana przy wykorzystaniu technik inżynierii społecznej, a w każdym systemie zarządzania cyberbezpieczeństwem najsłabszym ogniwem jest użytkownik systemu informatycznego. W artykule podjęto również próbę zdefiniowania pojęcia cyberbezpieczeństwo i zarządzanie cyberbezpieczeństwem. W tym celu została przeprowadzona analiza obowiązujących przepisów prawnych.

Autorzy dokonali również analizy cyberzagrożeń, na jakie narażone są małe i średnie przedsiębiorstwa oraz wskazali możliwości dalszych badań nad omawianą problematyką.

Słowa kluczowe: zarządzanie cyberbezpieczeństwem, zarządzanie kryzysowe, cyfrowe społeczeństwo, systemy teleinformacyjne, infrastruktura krytyczna

Statement of the problem in general outlook and its connection with important scientific and practical tasks

The digitisation of global economy contributes to the increasing cybernetic risk. The number of attacks is growing steadily. Cybercriminals turn to innovations to search for new areas and methods to acquire valuable assets belonging to various entities. Cybersecurity involves an “arms race” where attackers (intruders) and defenders fight against each other by limiting access to valuable resources. The assurance of cyber resilience forms part of proper management, and it can be achieved through raising the awareness of enterprise employees. Artificial Intelligence (AI) and Machine Learning (ML) are being applied in various spheres of industry, infrastructure and cities. If they are appropriately used in cybersecurity management, they may raise its effectiveness [1]. Cybersecurity protection has become a key task because of numerous instances of attacks, including hacker attacks and data breach incidents that caught the attention of the public. Effective cybersecurity protection involves not only the application of technical defence measures, such as firewalls or anti-virus software, but also the role of employees who have the knowledge of the ways to counter cyberattacks.

The proper functioning of contemporary societies, states and supra-national structures is, to a large extent, based on access to information. At the same time, technological advancement has encouraged most societies to move a substantial part of their operations and activities to the Internet (communication, online banking, tax office settlements, and access to various databases). Infrastructure management and control functions are also most often performed via the Internet. Therefore, one of the key tasks of public authorities is to ensure the digital security of societies. The functioning of information societies is based on ICT networks and systems. This makes societies extremely vulnerable to disruptions that affect their functioning. The threats to the IT sphere of societies have increasingly severe consequences, and cyberattacks may be used to exert economic or political pressure. In the event of major crises, operations in the IT space may constitute tools of influence supplementing traditional armed forces. The current times have been putting us to a test, with faster and more extensive transformation than ever before in the history of mankind. The multitude of information and the outburst of information technologies are powerful driving forces, changing all aspects of social, political, cultural and economic life. The effects of information revolution are particularly profound in the sphere of national security strategies. Most political phenomena and processes are reflected in cyberspace, and some of them are nowhere else to be found [2].

In practice, any disruption in the functioning of ICT networks might result in the unavailability of social services and the paralysis of the state. The absence of network access might result in a situation where it is not possible to access funds, where transport control systems and some medical services are disabled, and it is not possible to monitor power supply networks. In turn, disruptions in electricity supplies affect the operation of all critical infrastructure components.

Threats to the normal functioning of ICT networks and web services can have various sources. They include both the activities of malicious actors consisting in, for instance, unauthorised access to data and information, technical failures by fault of users or beyond their control, and physical damage to ICT infrastructure. In turn, the activities of malicious external actors may be based on exploiting the vulnerabilities of technical safeguards and the unawareness of cyberthreats resulting from insufficient levels of users' digital competencies. For these reasons, comprehensive cybersecurity management is one of the key elements assuring the secure and proper functioning of individuals, societies, states and other structures. In this context, cybersecurity management should be understood as the coordination of activities that are undertaken to provide the security of data, information systems and ICT networks. The notion also refers to the optimal use of resources aimed at taking action against a wide range of cyberattacks, including measures to counteract external cyberattacks. This refers not only to attacks via the Internet but also to those involving malware that may be placed, for

ISSN 2543-7097 / E-ISSN 2544-9478

DOI 10.5604/01.3001.0054.2880

example, in external data storage media. It should be noted, at this point, that unauthorised data access is possible even with devices that are not connected to the Internet, e.g., with the use of USB drives. This might result from both intentional actions and the lack of appropriate procedures having been developed or applied in practice.

In the context of cybersecurity management, emphasis should also be placed on the notion of information security, broadly understood as a measure to maintain the confidentiality, integrity and availability of information stored by enterprises and organisations. As per the ISO/IEC 27001 standard, information security management is not only related to the protection of information systems but it is also aimed at ensuring the security of personal data, commercial information and other information that constitutes trade secret. Furthermore, protection against information loss is a legal obligation imposed on all entities engaged in business operations, and its breach is punishable with severe criminal sanctions [3].

Cybersecurity management is a sphere of security management aimed at ensuring the proper functioning of digital society. The notion combines information security management, web service continuity management, and preparation for crisis situations. Therefore, it can be stated that cybersecurity management is an element of crisis management. These issues are significant due to the tense international situation and the growing level of threats arising from hostile activities in cyberspace. Such actions may be inspired by criminal groups, states or groups of states, and may be targeted against individuals, institutions, states or supra-national structures. Due to the technological progress and emerging threats, cybersecurity management requires continuous modifications. It is necessary to predict potential cyberthreats and to develop suitable methods to counteract them.

Analysis of latest research where the solution of the problem was initiated

The current state of research on cybersecurity management is dynamic and it continues to evolve in response to emerging threats, technologies and transformation in the digital environments and in the global balance of power. Cybersecurity management studies are most often conducted from the following points of view:

- Risk Management: research into the identification, assessment, management and monitoring of cybersecurity. This sphere includes both the technical aspects and risk management at the organisational level. These issues have been studied, *inter alia*, by Abdulmajeed Alahmari and Bob Duncan. Their research into cybersecurity management in small and medium-sized enterprises shows that such entities are turning to new technologies, such as cloud computing; however, in a vast majority of enterprises,

ISSN 2543-7097 / E-ISSN 2544-9478

DOI 10.5604/01.3001.0054.2880

there is no understanding of the actual cyberthreats, which in turns makes them increasingly vulnerable to such risks [4].

- Incident Management: a process aimed at effectively responding to security incidents to minimise damage and restore the normal operation of systems. In the context of cybersecurity, it includes incident identification, analysis and response, and the process of restoring systems to their normal state. Research into the methods of responding to cybersecurity incidents and related problems has been conducted, *inter alia*, by Marios Ioannou Eliana Stavrou and Maria Bada [5].
- Threat Intelligence: a study of effective methods for collecting, analysing and using threat intelligence to be better prepared to handle potential attacks. These issues have been studied, *inter alia*, by Martin Lee [6].

However, scholars have not conducted any studies that would adopt a comprehensive approach to cybersecurity management, including technical and social aspects of the issue in the context of cybersecurity management as a part of crisis management.

In Poland, cybersecurity is the object of research being conducted, *inter alia*, by Dariusz Prokopowicz who deals with the issues of electronic data exchange [7] and safe use of cyberspace by enterprises [8], whereas Andrzej Pieczywok studies the social aspects of counteracting threats in cyberspace [9], and their humanistic [10] and political [11] aspects.

Małgorzata Czuryk specialises in the legal aspects of cybersecurity. She analyses the status of local governments in that sphere [12], the observance of human rights and liberties in cyberspace [13], as well as cyberthreats in the context of declaring one of the states of exception [14]. She also deals with financial issues related to cybersecurity [15]. Paweł Pelc also examines the legal and financial aspects concerning cybersecurity [16]. Jarosław Kostrubiec [17], Krzysztof Gawkowski [18], Katarzyna Chałubińska-Jentkiewicz [19], and Piotr Milik [20] also focus on cybersecurity in their research.

Foreign scholars analysing threats in cyberspace include Istvan Hoffman [21], Miroslaw Kelemen [22], Oksana Evsyukova [23], and Andras Bencsik who explores the military aspects of cybersecurity [24], including the legal status of cyberarmies [25].

Aims of paper. Methods

The objective of the research was to analyse the possibilities to effectively develop a comprehensive cybersecurity management system. The analysis included data concerning digital competencies of societies, state digitisation levels, and cases of

ISSN 2543-7097 / E-ISSN 2544-9478

Karpiuk M., Pizło W., Kaczmarek K.,(2023). Cybersecurity Management – Current State and Directions of Change
International Journal of Legal Studies, 2(14)2023: 645 - 663
DOI 10.5604/01.3001.0054.2880

successful attacks. Only non-classified data were examined. Moreover, hypothetical emergency situations that might be caused by cyberattacks were analysed.

The main research method was literature review, supplemented by the hypothetico-deductive method.

As regards the legal aspects, two research models were applied: the doctrinal legal research method and the theoretical legal method. The doctrinal method was used to analyse legal regulations in terms of efficient cybersecurity management. The theoretical legal method allowed the assessment of actions aimed at ensuring proper cybersecurity management. Both methods are frequently used in legal studies.

Exposition of main material of research with complete substantiation of obtained scientific results. Discussion

Cybersecurity can be defined as a collection of measures adopted at a given enterprise, as well as tools, employees' expertise, and security strategies and concepts related to efforts aimed at minimising risks. The interdisciplinary nature of cybersecurity studies includes a wide range of knowledge of law, computer studies and, in particular, knowledge in the sphere of management. It is an area where the aspects of rules, technologies and human organisational behaviours are merged. In scientific literature, cybersecurity is described as the convergence of people, procedures and technologies to protect an organisation (enterprise), individuals (employees) or networks (an organisation's IT resources) against digital attacks and, in a broader sense, against third party interference. The issues refer to technical and organisational measures taken to protect digital resources of an organisation against unauthorised access or use [26]. The notion also refers to the following functions: risk management, insurance against cyberattacks or, in general terms, against interference of unauthorised persons in data systems in place at a given organisation. In addition to access control or "zero trust" policies [27], a potential strategy is to adopt offensive strategies that consist in searching for cybernetic threats and eliminating them in advance, before the organisation's data system is compromised [28]. Cybersecurity is defined as the convergence of human actions, procedures and technologies where the goal is to protect the cybernetic assets of an organisation and its employees against digital attacks. It is mainly about actions that are taken both in the technological and organisational sphere, with a view to securing digital assets against unauthorised third-party access or the unlawful use of such assets. The objective of the organisation is mainly to ensure security and uninterrupted functioning of web infrastructure, such as, for instance, computers, communication lines, software and data which form part and serve the purpose of using the Internet [26].

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

Cybersecurity is also described as a skill – the ability to protect the network, hardware and data against unauthorised access or illicit use, and the practice of ensuring confidentiality, integrity and availability of information [28]. The definitions highlight the multidimensional and interdisciplinary nature of cybersecurity, and demonstrate the need to adopt a holistic point of view on enterprise digital security systems. It is necessary to specify both the rules of operating in cyberspace in national and international dimensions, and in technical and managerial dimensions.

In literature, cybersecurity is defined as the protection of IT (Information Technology) and OT (Operational Technology) networks. IT includes technologies for the processing, storage, transmission and management of information, bringing together the activities of organisation managers on computers, computer networks, databases and software, the focus being on information security. OT, in turn, is focused on technologies and systems related to monitoring, controlling and managing physical production or operational processes. It is centred around such devices as sensors, industrial controls or industrial automation. The goal of OT is to effectively manage and control industrial operations, production, energy consumption and physical facilities. In the past few years, there has been a growing trend to integrate IT and OT as part of the IT/OT convergence concept. Such integration brings benefits for organisations, allowing them to better manage production and operational processes, while caring for the safety and integrity of IT systems and operational technologies.

The level of detail in cybersecurity management in an enterprise might differ, depending on the level of cybersecurity maturity that such organisation has managed to reach. Digital security management can be described as a collection of organisational resources, processes and its structures that might protect the organisation concerned, and entities cooperating with it [30] in cyberspace, against incidents that infringe their property rights. The level of organisations' preparedness for "intruder's" interference depends on the techniques at hand, and on the knowledge and competencies of the management staff. Individual levels of digital maturity of an organisation at the current stage of technological development, in the sphere of cybersecurity, can be specified as follows: level one [31] involves management staff's limited awareness of threats in cyberspace, taking provisional measures in the sphere of cybersecurity and the absence of any standard rules, procedures or threat control at various organisational levels; level two is characterised as a low risk-awareness level and involves the management staff having a basic knowledge of threats in cyberspace, implementing risk management processes and measures aimed at developing procedures and implementing policies for cybersecurity control; level three consists in formalising actions to audit

ISSN 2543-7097 / E-ISSN 2544-9478

DOI 10.5604/01.3001.0054.2880

system availability to intruders, standardising innovation procedures, and determining the scopes of cybersecurity control; level four involves an active, smart and fast response to threats affecting an organisation, including, in particular, the sphere of cybersecurity. The level also consists in the continuous monitoring of threats through mitigating the threats observed in information systems and adapting appropriate procedures to such threats. It should be stressed that the first level concerns digital security management at an organisation and includes a marginal level of knowledge of threats to the organisation's functioning. In turn, level four concerns proactive management, anticipating any potential threats. The activities that an organisation's management staff undertake include the anticipation of possible threats, introduction of safeguarding procedures, as it is the case with the "Zero trust" strategy.

Enterprises that manage digital security by adopting various types of action strategies may use specialist cybersecurity tools, designed to prevent unauthorised access to their networks, and these may include authentication procedures, firewalls and various access management systems [29]. As part of their strategies, enterprises can focus on managing cybersecurity procedures separately for IT and OT networks. They might also often decide to outsource some IT services to specialised data centres [32]. While searching for optimal solutions in the sphere of cybersecurity, enterprises invest considerable funds to ensure cloud data safety, to develop technologies to secure data and provide update functions, and to offer employee training [33]. Employees are a significant investment area, as the knowledge they gain at training courses, particularly in the field of cybercrime, efficiently improves information system security. Knowledge exchange takes place through sustained cooperation with academic circles. Active cybersecurity management in an enterprise entails employee education processes as a vital factor reducing the risk of negligence or omission in respect of cybersecurity of information systems [34]. Enterprise resources to boost cybersecurity resilience are also enhanced, and it is often effected through centralised management [26]. Decision-making functions are centred around strategic planning and proactive risk management policies. Organisational culture also undergoes transformation to promote active approaches to developing skills necessary to protect digital resources and combat cyberattacks. The management of risks related to information technology is often shifted to company board level. Investments in new information technologies, such as Machine Learning and Artificial Intelligence, are important areas of enterprise development. Enterprises search for state-of-the-art tools allowing the detection of intruder interference in the information systems of a given enterprise and any cooperating entities, as well as detection of malware and web traffic analysis [36]. Artificial

Intelligence and Machine Learning have found their place in digital security management, providing the ability to support the protection of systems against cyberattacks [37]. Good examples of using AI in cybersecurity management include web traffic analysis, detection of network intrusions, identification of malware and spam detection. The application of Artificial Intelligence can potentially reduce cyberthreat risk. It is possible to point to the following elements mitigating such threats [38], i.e., security system robustness, its response to threats, and resilience. The first element, the robustness of a cybersecurity system in an organisation is founded on the identification of the parts of an information system that remain stable in the face of adversarial attacks, which means that they can be subjected to self-testing and self-healing. The second element of the system is AI-based response through the ability to learn from every intruder interference or a direct attack targeting system components. AI is able to diagnose the type of "intruder activity" and boost defence capabilities, for example, through generating "baits" or honeypots. The latter are tools developed to attract cybercriminals and collect information on their methods, targets and attack techniques. The information collected through the honeypots may be used to refine safeguarding systems and adapt an organisation's security system in their policies. The third area of cybersecurity system stability is its resilience. Artificial Intelligence may help a cybersecurity system withstand an attack. Resilience can be based on a system of algorithms detecting cybernetic threats and identifying any anomalies.

Effective cyberattacks are mostly caused by one of the following factors:

- weak passwords and authentication: Users often use weak passwords or have the same passwords in multiple locations. If a password is compromised, the hacker may gain access to a lot of user's services,
- no software updates: outdated software, including operating systems, web browsers and applications, increases susceptibility to potential cyberattacks,
- no anti-virus and anti-malware safeguards: not having such software or not updating it regularly increases the risk of infecting the device with malware.
- no cybersecurity training: awareness of cybersecurity is critical, as otherwise users are prone to phishing or social engineering attacks.
- failure to observe the principle of least privilege (PoLP): the provision of excessive authorisation to users might result in facilitating access to important data; particularly when the attack is targeted against a user with excessive authorisation,
- no network monitoring: insufficient network monitoring might mean that an attack remains unnoticed for a long time, allowing unauthorised persons to move around the affected system freely,

ISSN 2543-7097 / E-ISSN 2544-9478

DOI 10.5604/01.3001.0054.2880

- improper security system configuration: improper firewall configuration, no appropriate access rules or improper configuration of safeguarding systems may open doors for potential attackers,
- no back-up: if an organisation does not generate back-up copies regularly, it is likely to become more vulnerable to ransomware attacks,
- known system vulnerabilities: hackers often exploit known vulnerabilities in the software which has not been updated yet, in order to gain access to systems,
- no coordinated incident response plan: organisations that do not have a clear incident response plan may encounter obstacles in providing fast and effective response to cyberattacks.

The results of analyses show that users are the weakest link of cybersecurity management. This does not need to result from the low level of digital skills, but may be the outcome of ignoring safety procedures and rules. This, in turn, may be caused by routine. Another factor that can weaken cybersecurity management systems includes disruptions in both horizontal and vertical information flows. The causes of such disruptions can also be attributed to users.

As regards the context of normative conditions of cybersecurity, the Polish legislator regulated the issues of cybersecurity in the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws of 2023, item 913, as amended), hereinafter referred to as the NCSA. The Act also includes the definition of cybersecurity which, under Article 2 (4) of the NCSA, is understood as the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems. The legislator refers to ensuring the protection of information systems, which comprise ICT systems and the data processed there. As per Article 3 (3) of the Act of 17 February 2005 on the Computerisation of Entities Performing Public Tasks (consolidated text, Journal of Laws of 2023, item 57, as amended), an ICT system is defined as a set of cooperating IT hardware and software, providing a possibility to process and store, as well as send and receive, data via ICT networks with the use of an end device suitable for a given network type. As regards the military sphere, the armed forces operate the military telecommunications systems which, under Article 17(1) of the Homeland Defence Act of 11 March 2022 (consolidated text, Journal of Laws of 2022, item 2305, as amended), ensures telecommunication activities for: (1) organisational entities and units, including military units during their deployment or stay outside the territory of Poland; and (2) organisational units of foreign armed forces or foreign state authorities temporarily staying on the territory of the Republic of

ISSN 2543-7097 / E-ISSN 2544-9478

DOI 10.5604/01.3001.0054.2880

Poland under agreements to which Poland is a party, if relevant technical capabilities are available.

The management of ICT systems, notwithstanding whether they are public, military or civilian, requires qualified staff that not only have suitable expertise in cybersecurity management and effectiveness of such systems, but also skills allowing them to apply that expertise and effectiveness in practice. The personnel will need to take actions which, on the one hand, allow a wide access to services rendered in cyberspace, and, on the other hand, provide security against interference into the normal functioning of ICT systems through which the services are provided. Professional staff members are the foundation of efficient cybersecurity management, no matter the sphere it occurs in.

In Article 2(4) of the NCSA, the Polish legislator defines cybersecurity as the resilience of information systems to actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems. Therefore, cybersecurity management needs to entail all these elements, namely the confidentiality, integrity, availability and authenticity of the processed data or related services, though not always in the same extent, depending on the nature of the services, the categories of information being processed (public, personal, confidential, or commercial data), and the threat that might infringe the operation of an ICT system, or even paralyse it. It also depends on the damage that the disruption may cause.

The NCSA refers to incident management (under Article 2 (5) of the NCSA, an incident is understood as a phenomenon which has or might have a negative effect on cybersecurity) and risk management (under Article 2 (12) of the NCSA, risk is defined as a combination of probability of an adverse event and its consequences).

Under Article 2 (18) of the NCSA, incident management (as an element of cybersecurity management) is understood as incident handling, identification of links between incidents, elimination of incident causes, and the development of conclusions arising from incident handling operations. Given the above, incident management is related to its handling, which is defined, under Article 2 (10) of the NCSA, as activities allowing incident detection, recording, analysis, classification, prioritisation, the adoption of remedial measures, and mitigation of incident impact. Incident management is related to both countering and eliminating cyberattacks, and removing their outcomes. It includes preventive, ongoing, and follow-up actions. This corresponds to three stages of cybersecurity management related to the fight against the negative events in cyberspace.

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska
This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)
Karpiuk M., Pizło W., Kaczmarek K.,(2023). Cybersecurity Management – Current State and Directions of Change
International Journal of Legal Studies, 2(14)2023: 645 - 663
DOI 10.5604/01.3001.0054.2880
655

Under Article 2 (19) of the NCSA, risk management is understood as coordinated actions in the sphere of cybersecurity management in relation to estimated risks. As regards risk management forming part of cybersecurity management, the prediction, identification and analysis of risk should be taken into account, together with the consequences that such risk may have.

In legal terms, cybersecurity management needs to take into account the fulfilment of the objective laid down in Article 3 of the NCSA, which is to ensure cybersecurity at the national level, which entails the uninterrupted provision of essential services and digital services through reaching an appropriate level of security of the information systems used to render these services and through ensuring incident handling operations. In this aspect, cybersecurity management refers to three elements: uninterrupted provision of essential services, uninterrupted provision of digital services, and incident handling.

Under Article 2 (16) of the NCSA, an essential service is a service which is essential for the maintenance of critical societal and/or economic activities, entered in the list of essential services. Under Article 8 of the NCSA, operators of essential services are obliged to put in place a security management system within the information system used for providing a given essential service. The objective is to be achieved through: (1) maintaining regular risk assessment for incident occurrence and managing such risks; (2) implementing appropriate and proportional technical and organisational measures for risk assessment, taking into account the state-of-the-art; (3) collecting information about cybersecurity threats and vulnerabilities in the information systems used for providing essential services; (4) providing incident management; (5) applying measures to prevent and mitigate the impact of incidents on the security of the information systems used for providing essential services; and (6) applying means of communication to allow suitable and safe contacts as part of the national cybersecurity system. At the level of essential service provision, cybersecurity management must take into account all the above-mentioned aspects in order to be effective and to protect the ICT systems used by operators of essential services against cyberthreats and their consequences.

Cybersecurity management, in the context of essential service management, is also related to crisis management. Owners, owner-like possessors or lessees of facilities, installations, and devices which constitute critical infrastructure are obliged to protect them, as laid down in Article 6 (5) of the Crisis Management Act of 26 April 2007 (consolidated text, Journal of Laws of 2023, item 122, as amended), in particular through preparing and implementing critical infrastructure protection plans in line with

ISSN 2543-7097 / E-ISSN 2544-9478

DOI 10.5604/01.3001.0054.2880

the anticipated threats, and maintaining their own back-up systems to ensure security and the continued functioning of the infrastructure, until it is restored in full to its working order. If they are, at the same time, operators of essential services, they have additional cybersecurity obligations, including the proper cybersecurity management. The objective of crisis management is, *inter alia*, to protect critical infrastructure against threats that might impact its functioning. The operation of critical infrastructure that relies on ICT systems might be disrupted by cyberthreats. Therefore, its protection must take into account cybersecurity rules which allow its proper functioning, which means that it is not only about predicting, counteracting and eliminating threats, but also about removing the damage caused by adverse events [39]. Cybersecurity management should also take into account the protection of critical infrastructure that contributes to the stability of the state and economy.

Under Article 2 (15) of the NCSA, a digital service means a service provided by electronic means, as listed in the Annex to the NCSA. In line with the definition set out in Article 2 (4) of the Act of 18 July 2002 on the Provision of Services by Electronic Means (consolidated text, Journal of Laws of 2020, item 344, as amended), the provision of services by electronic means is defined as the provision of a service without a simultaneous presence of the parties (remotely), through the transfer of data at the customer's individual request, transmitted and received with the use of electronic data processing devices, including digital compression and data storage, and fully sent, received and transmitted via a telecommunications network. Digital services include the following services provided by electronic means: (1) an online marketplace – a digital service that allows consumers and/or traders to conclude online sales or service contracts with traders, either on the online marketplace's website or on a trader's website that uses the services provided by the online marketplace; (2) a cloud computing service – a digital service that enables access to a scalable and flexible pool of computing resources shared by multiple users; and 3) an online search engine – a digital service that allows users to perform searches of all websites, or websites in a particular language, on the basis of a query in the form of a keyword, a phrase or other input, displaying links in which information related to the requested content can be found. Under the NCSA, cybersecurity management related to the assurance of an uninterrupted provision of digital services concerns three types of services, i.e., online marketplaces, online search engines and cloud computing services. As a rule, it covers the private sector and the national cybersecurity system developed alongside the public sector. Therefore, cybersecurity management will also need to have a systemic dimension, whereby cybersecurity is perceived as a global phenomenon, instead of merely something that is guaranteed locally by individual entities responsible for the security of the ICT systems they hold. It will also need to take into consideration the priorities and tasks shared across the system and similar organisational solutions. The actions to be taken in the sphere of cybersecurity management will not always be the same at various levels and stages, which is directly related to an existing or potential threat, and the reach and hardship of its consequences, if such threat has indeed occurred.

Numerous scholars point to the fact that centralised management significantly contributes to reducing the risk of "intruder's" interference in the information security system in place at a given organisation. Small and medium-sized enterprises (SMEs) are regarded as entities that are particularly exposed to cybercrime threats. They are the most immature and not resilient to emergency situations. The need for investments in cybersecurity technologies should be taken into consideration to mitigate the risk for SMEs. Cooperation and information exchange between enterprises play a vital part in efforts to counter cyberthreats. Another vital factor in reducing the risk of cyberattacks is to have proper infrastructural resources to improve system security and decrease the frequency of security incidents.

In the macro sphere, a need for creating international cooperation networks has been indicated [29], with a view to exchanging information and resolving cybersecurity issues at national, regional and civic levels. Politicians should implement cybersecurity models [40] to gain citizens' trust and engage them in the development of a system for the protection of financial and personal data systems. Educational initiatives in this sphere are vital to solve the problem of insufficient employees' cybersecurity skills [32]. The engagement of multiple entities in cybersecurity [41] may boost the use of information and communication technologies in enterprises, and improve management conditions. The improved protection, coupled with education in the field of cybersecurity, might contribute to creating as safer and more productive space for utilising new technologies [42]. The security of information systems can increase the investment attractiveness of economy sectors where regulatory authorities place particular emphasis on security conditions. Cybersecurity education programmes should be tailored to students' preparation levels and labour market needs, in order to solve the problem of continued shortages of cybersecurity staff [43].

Conclusion

In numerous publications, enterprise size is quantified in various ways, taking into account the number of employees, the total value of assets, market potential, etc. However, there are no studies on the issue of "enterprise size" and the impact of security

ISSN 2543-7097 / E-ISSN 2544-9478

DOI 10.5604/01.3001.0054.2880

breach events in an organisation on stock value fluctuations. Every attack, for example, a hacker attack or data loss, results in the reduction of trust to the attack victim. It is advisable to conduct research that would be aimed at defining not only the technological deficiencies in safeguards but also the consequences for proper management and the economic outcomes of third-party interference. The analysis of the effects of introducing legal regulations on security events and their consequences might constitute the basis for future laws and motivate states that fall behind in terms of enacting relevant provisions. In addition, the results of the study confirm that the negative consequences of security breach incidents are usually less burdensome for the shareholders of large companies, compared with smaller entities.

ICT systems, particularly those that are responsible for the stability of the state and its economy, must be duly protected. They also play a vital role in society, so their reliability and security must be a priority in the activities of entities responsible for the functioning of the systems, which refers to both the public and the private sector [44]. Cybersecurity is thus a major part of public policies and private business operations based on cyberspace. Both sectors (private and public) need to implement cybersecurity management systems in their activities, allowing them to operate ICT systems that are resilient to cyberattacks.

It should be stressed that the state is engaged in the development of information society, which also triggers the need to ensure cybersecurity, and which is reflected, *inter alia*, in investing in the development of information technologies, including administration itself, in the sphere of contacts with citizens, and also in respect of funding the construction and upgrades of telecommunications infrastructure. These actions are aimed at solving the related issues. They include eliminating digital exclusion, protecting consumers in electronic trade, combating cybercrime, developing electronic payment systems, respecting the privacy of individuals, and protecting intellectual property rights [45].

Cybersecurity management should take into account the objectives set out in the Cybersecurity Strategy of the Republic of Poland for 2019-2024, adopted by the Council of Ministers on 22 October 2019 (Official Gazette of the Republic of Poland of 2019, item 1037). These include the main objective, i.e., to improve the level of resilience to cyberthreats and to increase the level of information protection in the public, military and private sectors, and to promote knowledge and good practices helping citizens to better protect their information, as well as specific objectives, i.e., to develop the national cybersecurity system, to increase the level of resilience of information systems operated by public administration and the private sector, and to provide capability to effectively prevent and respond to incidents; to boost the national potential in the sphere of security in the cyberspace; to raise awareness and social competences in the sphere of cybersecurity; and to build a strong international position of the Republic of Poland in the sphere of cybersecurity.

In the context of tense international situation, climate change, and the likelihood of extreme weather conditions or energy crisis, the potential physical damage to ICT and power supply infrastructure should also be taken into consideration. In such cases, the functioning of societies based on access to information may be disrupted. It seems to be a considerable challenge to prepare societies for such circumstances. In the context of cybersecurity management, it is important to have a working back-up power source, in particular in the case of network service providers, as a sudden power outage may result in system failure and the inability to restart the system after electricity supply is resumed.

As regards further research into cybersecurity management systems, the key issue seems to be to conduct analyses concerning users susceptibility to cyberthreats, in particular attacks based on social engineering. This particularly refers to management staff and board members in organisations, as they have access to the critical points of information systems. It can be assumed that individuals in managerial positions (and their devices) are most often used to get unauthorised access to information systems. Therefore, from the perspective of cybersecurity management, individuals managing organisations and institutions should be required to take part in cybersecurity training.

It is also advisable to conduct analyses concerning the conformity of cybersecurity management procedures with the actual circumstances.

References

1. Schmitt M. Artificial Intelligence in Business Analytics: Capturing Value With Machine Learning Applications in Financial Services, Doctoral Thesis, University of Strathclyde, 2020, https://doi.org/10.48730/5s00-jd45.
2. Kaczmarek K. Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii. *Cybersecurity and Law*, 2019; 1:143-157.
3. Polskie Centrum Badań i Certyfikacji. Czym jest System Zarządzania PN-EN ISO/IEC 27001. https://www.pcbc.gov.pl/pl/uslugi/certyfikacja-systemow-zarzadzania/pluslugicertyfikacja-systemow-zarzadzaniapn-iso-iec-27001 (3 December 2023, date last accessed)

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

4. Alahmari A., Duncan B. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence, 2020 *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA*), Dublin, 2020: 1-5.
5. Ioannou M., E., Bada M. Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination, *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),* Oxford, 2019: 1-4.
6. Lee M. *Cyber threat intelligence*. John Wiley & Sons, New Jersey 2023.
7. Gwoździewicz S., Prokopowicz D. Determinants of Electronic Data Interchange Security in the Context of Big Data and Cloud Computing Technology Development. Sentiment Analysis Conducted for Cybercrime Issues Occurred in the Period from May 2017 to February 2019. *International Journal of New Economics and Social Sciences* 2022, 1: 70-109.
8. Prokopowicz D., Matosek M. Importance And Security Of Information Provided By The Internet In The Context Of The Development Of Economic Entities In Poland. *International Journal of New Economics and Social Sciences* 2017, 2: 219-229.
9. Pieczywok A. The use of selected social concepts and educational programmes in counteracting cyberspace threats. *Cybersecurity and Law* 2019, 2: 61-74.
10. Pieczywok A. Cyberspace as a source of dehumanization of the human being. *Cybersecurity and Law* 2023, 1: 40-47.
11. Pieczywok A. Polityczno-prawne strategie i dyrektywy przeciwdziałania cyberzagrożeniom. *Cybersecurity and Law* 2023, 2: 156-166.
12. Czuryk M. Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity. *Cybersecurity and Law* 2019, 2: 39-50.
13. Czuryk M. Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues. *Studia Iuridica Lublinensia* 2022, 3: 31-43.
14. Czuryk M. Cybersecurity as a premise to introduce a state of exception. *Cybersecurity and Law* 2021, 2: 83-90.
15. Czuryk M. Special rules of remuneration for individuals performing cybersecurity tasks. *Cybersecurity and Law* 2022, 2: 105-112.
16. Pelc P. Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa. *Cybersecurity and Law* 2019, 2: 151-164.
17. Kostrubiec J. The position of the Computer Security Incidents Response Teams in the national cybersecurity system. *Cybersecurity and Law* 2022, 2: 27-35.
18. Gawkowski K, Cyberbezpieczeństwo w inteligentnym mieście. *Cybersecurity and Law* 2023, 2: 95-105.
19. Chałubińska-Jentkiewicz K. *Cyberodpowiedzialność*, Toruń: Wydawnictwo Adam Marszałek, 2019.

ISSN 2543-7097 / E-ISSN 2544-9478

DOI 10.5604/01.3001.0054.2880

20. Milik P. International legal regulations in the area of cybersecurity. *Cybersecurity and Law* 2019, 1: 115-141.
21. Hoffman I., Karpiuk M. The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary. *Cybersecurity and Law* 2021, 1: 171-190.
22. Karpiuk M., Kelemen M. Cybersecurity in civil aviation in Poland and Slovakia. *Cybersecurity and Law* 2022, 2: 70-83.
23. Evsyukova O. Political digitalization for Ukrainian society – challenges for cybersecurity. *Cybersecurity and Law* 2021, 1: 139-144.
24. Bencsik A., Karpiuk M. Cybersecurity in Hungary and Poland. Military aspects. *Cybersecurity and Law* 2023, 1: 82-94.
25. Bencsik A., Karpiuk M. The legal status of the cyberarmy in Hungary and Poland. An overview. *Cybersecurity and Law* 2023, 2: 19-31.
26. Hasani T, O'Reilly N, Dehghantanha A, Rezania D, Levallet N. Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Bus Econ*. 2023,3(5):97. doi: 10.1007/s43546-023-00477-6.
27. Pizło W. Management in Cyberspace: From Firewall to Zero Trust. In: Karpiuk M., Kostrubiec J., (eds.), *The Public Dimension of Cybersecurity*, Maribor, Institute for Local Self-Government Maribor, 2022: 133-146.
28. Heeren-Moon E. Risk, reputation and responsibility: Cybersecurity and centralized data in United States civilian federal agencies. *Telecommunications Policy*, Volume 47, Issue 2, 2023, https://doi.org/10.1016/j.telpol.2023.102502.
29. Chang K., Huang, H. Exploring the management of multi-sectoral cybersecurity information-sharing networks. *Government Information Quarterly*, Volume 40, Issue 4, 2023, https://doi.org/10.1016/j.giq.2023.101870
30. Pizło W., Parzonko A. Virtual Organizations and Trust in: Trust, Organizations and the Digital Economy. Theory and Practice, Paliszkiewicz J., Chen K., (red.), 2022, Taylor & Francis Group 2022: 61-78.
31. Kurnianto V., Hidayat G. 2023, A Comprehensive Cybersecurity Maturity Study for Nonbank Financial Institution. *Journal of System and Management Sciences* Vol. 13 No. 5, 2023: 525-543, DOI:10.33168/JSMS.2023.0534.
32. Jiang, Y., Jeusfeld, M.A., Ding, J. et al. Model-Based Cybersecurity Analysis. Bus Inf Syst Eng 65, 2023: 643–676, https://doi.org/10.1007/s12599-023-00811-0
33. Dinkova, M., El-Dardiry, R. & Overvest, B. Should firms invest more in cybersecurity?. *Small Bus Econ* (2023). https://doi.org/10.1007/s11187-023-00803-0
34. Héroux, S., Fortin, A. Board of directors' attributes and aspects of cybersecurity disclosure. *J Manag Gov* (2022). https://doi.org/10.1007/s10997-022-09660-7
35. Georg-Schaffner, L., Prinz, E. Corporate management boards' information security orientation: an analysis of cybersecurity incidents in DAX 30 companies. J Manag Gov 26, 1375–1408 (2022). https://doi.org/10.1007/s10997-021-09588-4

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

36. Schmitt M., Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection, Journal of Industrial Information Integration, Volume 36, 2023, https://doi.org/10.1016/j.jii.2023.100520
37. Sarker I.H., Furhad M.H., Nowrozy R., AI-Driven Cybersecurity, An overview, security intelligence modeling and research directions, SN Comput. Sci. 2 (2021) 1–18, https://doi.org/10.1007/s42979-021-00557-0.
38. Taddeo M., McCutcheon T., Floridi L., Trusting artificial intelligence in cybersecurity is a double-edged sword, Nat. Mach. Intell. 1 (2019) 557–560, https://doi.org/10.1038/s42256-019-0109-1.
39. Karpiuk M., Crisis management vs. cyber threats. *Sicurezza, Terrorismo e Societa* 2022, 2: 113-123.
40. Daniel, C., Mullarkey, M. & Agrawal, M. RQ Labs: A Cybersecurity Workforce Skills Development Framework. *Inf Syst Front* 25, 431–450 (2023). https://doi.org/10.1007/s10796-022-10332-y
41. Krishna B., Krishnan S., 2022 'Examining the Relationship between National Cybersecurity Commitment, Culture, and Digital Payment Usage: An Institutional Trust Theory Perspective', Information Systems Frontiers, 25, 1713 – 1741
42. Ahangama S., 2023 'Relating Social Media Diffusion, Education Level and Cybersecurity Protection Mechanisms to E-Participation Initiatives: Insights from a Cross-Country Analysis', Information Systems Frontiers, 1 - 17
43. Clinton D., Matthew T. Mullarkey, 2022 'RQ Labs: A Cybersecurity Workforce Skills Development Framework', Information Systems Frontiers, 1 - 20
44. Bencsik A., Karpiuk M., Kelemen M., Włodyka E., *Cybersecurity in the Visegrad Group Countries*, Maribor: Lex Localis Press, 2023: 89-90.
45. Tyrawa D., Krajowy system cyberbezpieczeństwa w świetle nauki prawa administracyjnego. Uwagi wybrane. *International Journal of Legal Studies* 2023, 1: 13-30.

ISSN 2543-7097 / E-ISSN 2544-9478

DOI 10.5604/01.3001.0054.2880