European Research Studies Journal
Volume XXVII, Issue 2, 2024

pp. 454-464

How Cybersecurity Shapes Effective Organizational Management

Submitted 08/04/24, 1st revision 26/43/24, 2nd revision 10/05/24, accepted 06/06/24

Zbigniew Ciekanowski[1], Julia Nowicka[2], Mariusz Czternastek[3], Sławomir Żurawski[4], Piotr Mikosik[5]

Abstract:

Purpose: *The main purpose of this article is to analyze the role of cybersecurity in the management of a modern organization. The article addresses the issue of security management within an organization to highlight the area of cybersecurity, which presents new challenges due to the rapid development of technology and emerging threats in cyberspace.*
Design/Methodology/Approach: *The main research problem is formulated as follows: How does the level of cybersecurity affect the functioning of an organization? The study utilizes the latest research presented in documents and reports on cybersecurity, published in 2023 by international and national organizations and institutions. Additionally, an analysis was conducted based on scientific articles from recent years. Information was also obtained from national legal acts and documents published by European Union bodies.*
Findings: *Cybersecurity management is a crucial element of the functioning of a modern organization. Organizations that do not take action in the field of cybersecurity risk not only financial losses or loss of reputation but also the possibility of ceasing operations.*
Practical Implications: *Cybersecurity plays a key role in managing a modern organization, protecting the company's data, systems, reputation, and financial resources. In the face of the increasing number and complexity of threats, organizations must constantly adapt their security strategies. An effective cybersecurity strategy can protect against significant financial losses, loss of reputation, and legal consequences. Moreover, it can help build trust among customers and business partners, which is essential for the long-term success of the organization. Cyber threats are constantly evolving, requiring continuous monitoring and analysis of new trends and techniques used by cybercriminals. Continuous research on new threats, including research on specific industries and sectors, is needed to create dedicated protection strategies.*

[1]*Faculty of Economics, John Paul II University of Applied Sciences in Biała Podlaska, Poland, ORCID: 0000-0002-0549-894X, zbigniew@ciekanowski.pl;*
[2]*War Studies University, Poland, ORCID: 0000-0002-0778-0519, j.nowicka@akademia.mil.pl;*
[3]*University of the National Education Commission Krakow, Poland; ORCID: 0000–0002–0396–9904; mariusz.czternastek@up.krakow.pl;*
[4]*State School of Higher Education in Chełm, Poland, ORCID: 0000-0001-9527-3391, slawomir.zurawski@onet.pl;*
[5]*Warsaw Management University, Poland, ORCID: ORCID 0000-0003-0056-7990, e-mail: piotr.mikosik@mans.org.pl;*

Originality/Value: *In this study, the authors characterize the security environment within an organization, describe the cybersecurity framework for organizations in both EU and Polish legal regulations, and present contemporary cybersecurity threats within organizations. Continuous research and implementation of the latest protection technologies, such as artificial intelligence (AI) and machine learning (ML), which can predict and detect new types of threats, are necessary. Further research on the application of AI and ML in cybersecurity can significantly improve an organization's ability to respond quickly to threats.*

Keywords: *Cybersecurity, cyberspace, management, organization, threats.*

JEL codes: *K24, M10, M15.*

Paper type: *Research article.*

1. Introduction

Modern organizations increasingly rely on information technology in conducting their activities. The use of advanced computer systems, networks, and mobile devices has become an indispensable element of the functioning of enterprises worldwide.

Along with the growing dependence on information technology, the risk associated with cyberattacks also increases. Cybercrime is becoming more sophisticated, and attacks are more coordinated and targeted, posing a serious threat to data security and the continuity of organizational operations.

Cybersecurity is a key element of organizational management in the digital age. It encompasses the protection of information systems, networks, programs, and data from attacks, damage, or unauthorized access. Managing the risk associated with cybersecurity is not only a technological issue but also a strategic one. It requires engagement at all levels of the organization, from the board of directors to managers and down to the rank-and-file employees.

The importance of cybersecurity for organizations cannot be overstated. An effective cybersecurity strategy can protect against significant financial losses, reputational damage, and legal consequences. Furthermore, it can also contribute to building trust among customers and business partners, which is crucial for the long-term success of the organization.

This study will discuss the role of cybersecurity in organizational management. The main cyber threats faced by modern enterprises and the methods and tools used to protect against these threats will be presented.

Attention will also be drawn to the importance of creating a security culture within the organization and the necessity of continuously improving cybersecurity strategies in response to changing threats.

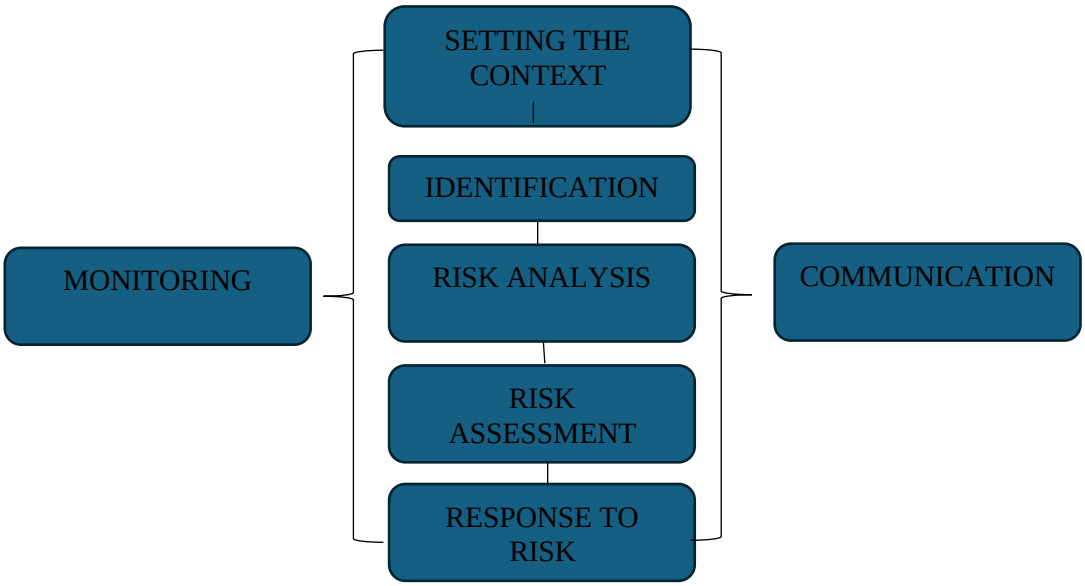
2. Security Environment in the Organization

In the era of intensive development of information technology, organizations must face the growing risk associated with cyber threats. The security environment in the organization includes all measures, procedures, and mechanisms aimed at protecting its information resources and ensuring continuity of operations.

Creating and maintaining an effective security environment is crucial for any organization, regardless of its size or industry (Loishyn *et al.*, 2021). The foundation of any security environment is a clearly defined information security policy. This document outlines the rules and procedures for data protection, access control, and risk management (Shuliak and Shuliak, 2020).

The policy should comply with applicable legal regulations and industry standards. A key aspect is also the identification, assessment, and management of risk, including that associated with cyber threats. Below are the stages of the risk management process in the organization.

Figure 1. *Stages of the risk management process in an organisation.*



Source: *Wojtyto, 2019.*

Organizations must conduct regular risk analyses to identify potential threats and develop appropriate countermeasures. Effective management of access to

informational resources is indispensable. Organizations must implement access control mechanisms that ensure only authorized individuals have access to sensitive data and systems (Wojtyto, 2019). It is important to apply the principle of least privilege and regularly review permissions.

People are the weakest link in the security chain. Regular training and raising employee awareness about cyber threats and best practices in information security are crucial for creating a security culture within the organization (Szafranek, 2021).

Implementing advanced security technologies, such as firewalls, intrusion detection systems (IDS), antivirus software, and data encryption, is essential for protection against cyberattacks. Organizations should also regularly update their systems to protect against new threats.

An effective security environment must include well-defined incident response procedures. Organizations should be prepared to quickly and effectively respond to security breaches, minimizing their impact on operations and preventing future incidents.

Creating and maintaining an effective security environment is crucial for protecting an organization's informational resources and ensuring its continuity of operations. In the era of increasing cyber threats, investing in cybersecurity is not only a necessity but also a strategic step that can bring tangible benefits. Organizations that effectively manage their security environment gain a competitive advantage by building trust among customers, business partners, and other stakeholders.

Conclusions from the analysis of the security environment in an organization show that an effective cybersecurity strategy requires a holistic approach, taking into account both technological and human aspects. Only then is it possible to create an environment that effectively protects against threats and enables the safe functioning of the organization in the digital world.

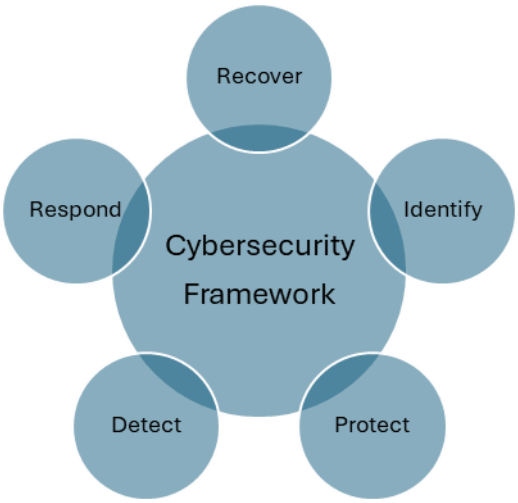
3. Cybersecurity Frameworks for Organizations

In the face of increasing cyber threats, organizations must implement comprehensive cybersecurity frameworks that include strategies, policies, procedures, and technologies for protecting informational resources. Below are key frameworks and standards that help organizations create effective cybersecurity programs. CSF functions provide guidelines for the actions outlined below.

This five-function model in Figure 2 offers a comprehensive view of an organization's cyber risk management throughout its lifecycle (https://seqred.pl/zalozenia-ramowe-cyberbezpieczenstwa-identyfikacja/).

The National Institute of Standards and Technology (NIST) cybersecurity framework provides organizations with a systematic approach to understanding, managing, and mitigating cybersecurity risks, thereby improving their overall cybersecurity posture https://www.ssl.com/pl/artyku%C5%82/szczeg%C3%B3%C5%82owe-om%C3%B3wienie-nistowych-ram-cyberbezpiecze%C5%84stwa/.

Figure 2*. CSF Functions*



Source: *The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology.*

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is one of the most recognized standards in the world. The following are the essence of the five key functions:

1. Identify: Understand the organizational context, resources, and risks associated with cybersecurity.
2. Protect: Protect critical services and infrastructure by implementing appropriate security measures.
3. Detect: Identify the occurrence of security incidents.
4. Respond: Respond quickly to incidents to minimize their impact.
5. Recover: Restoring normal operations after incidents and implementing corrective actions (The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology).

Creating and maintaining an effective cybersecurity framework is essential to protect an organization's information assets and ensure business continuity (Levy, 2015). Adopting and implementing appropriate standards and best practices, such as the NIST Cybersecurity Framework, can significantly improve the level of security in an organization.

The Polish equivalent of this document is the "Framework for Risk Management in Organizations and Information Systems". They are a recommendation in the form of National Cybersecurity Standards. Although the presented standards have been developed on the basis of publications of the American National Institute of Science and Technology (NIST), they have a mapping to the Polish Standards in force in the Polish legal system, used in information security management by entities of the national cybersecurity system (Risk Management Framework in Organizations and Information Systems. Security and privacy in the system lifecycle, 2021).

Risk Management Framework (RMF). RMF consists of seven stages; preparatory stage, which is to ensure that the organisation is ready to implement the process, and six main stages. All seven stages are shown in Figure 3.

Figure 3. *Risk Management Framework – RMF*

Source: *Framework for Risk Management in Organizations and Information Systems. Security and Privacy in the System Lifecycle, 2021*.

Risk management is a process that underpins the management of organizations, teleinformatics systems, and areas of business or administrative activities (Roszyk-Kowalska et al. 2023). Risk management activities in organizations have developed particularly dynamically in recent years, especially in the area of cybersecurity (Mąkosa, 2019).

Risk management frameworks are a structural approach that allows organizations to identify, assess, manage, and monitor risks associated with their operations,

including IT systems. Implementing effective risk management frameworks helps protect organizational resources, ensure business continuity, and meet legal and regulatory requirements.

Risk management frameworks in organizations and IT systems, along with the NIST Cybersecurity Framework 2.0, offer complementary approaches to managing cybersecurity risk. Both structures emphasize threat identification, resource protection, incident detection, response, and recovery of operational capabilities, helping organizations effectively manage risk and protect against cyber threats.

4. Cybersecurity Threats in Organizations

Cybersecurity in organizations is exposed to various threats that can have serious consequences for the integrity, confidentiality, and availability of information systems. Analysing cybersecurity incidents is a key element of risk management and threat response.

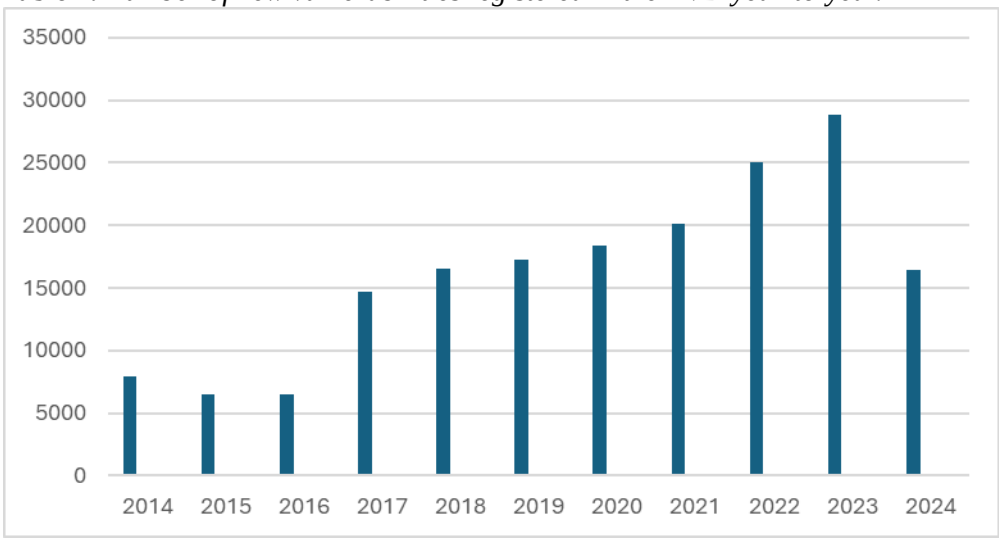
CERT Polska is a Computer Emergency Response Team operating within the NASK structures. Since the team's inception, its core activity has been handling security incidents and collaborating with similar units worldwide in both operational and research-implementation spheres. The main tasks of the CERT Polska team include:

The CERT Polska team is a Computer Emergency Response Team operating within NASK. From the beginning of the team's existence, the core of its activity has been the handling of security incidents and cooperation with similar units around the world, both in the sphere of operational activities and research and implementation (CERT Polska):

- recording and handling events that violate network security,
- proactive response in the event of direct threats to users,
- cooperation with other CERT teams in Poland and around the world,
- participation in national and international projects related to ICT security, research activities in the field of methods of detecting security incidents, malware analysis and threat information exchange systems,
- developing own tools for detecting, monitoring, analysing and correlating threats,
- regular publication of the CERT Polska report on the security of Polish Internet resources,
- information and educational activities aimed at increasing awareness of ICT security, including: publishing information about security on the cert.pl blog and on Facebook and Twitter social networking sites, organization of a cyclical SECURE conference, independent analyses and tests of ICT security solutions (Office of the Polish Financial Supervision Authority).

As CERT Polska rightly pointed out, such a drastic increase in the scale of cyber incidents, especially on critical infrastructure entities, let us remind you about 178 percent, resulted from the outbreak of an armed conflict across our eastern border. The number of new vulnerabilities registered in the NVD database on an annual basis is presented below.

Table 1. *Number of new vulnerabilities registered in the NVD year-to-year.*



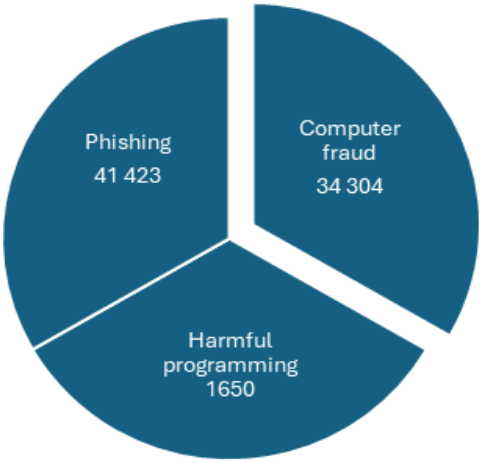
Source:*https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&&results_type=statistics&&-search_type=all&&isCpeNameSearch=false*

In 2023, there was an increase in the number of new vulnerabilities. More than 29 thousand new vulnerabilities were published in the National Vulnerability Database, which is maintained by the American agency NIST (NIST). Particular attention should also be paid to CISA statistics from the database of known and exploited vulnerabilities (CISA) which allow for a more accurate assessment of the current threat landscape.

At the end of 2023, 1074 different vulnerabilities were actively exploited, of which 137 were vulnerabilities published in the same year. For comparison, in 2022 it was 868 and 92 vulnerabilities, respectively. The CERT Polska team actively monitored vulnerabilities in products that are widely used in Poland.

If the Team obtained, as part of its own or from the partner, information about a vulnerable instance of the product, it established communication with vulnerable entities to implement the necessary updates and mitigate potential risk (Report CERT Polska 2023). The following are the most common types of incidents in Poland in 2023 according to the CERT Polska report.

Figure 4. *The most common types of incidents in 2023 in Poland*



Source: *https://cert.pl/uploads/docs/Raport_CP_2023.pdf.*

The most common type of incidents recorded in 2023 were, as has been the case for many years, phishing websites. Another prevalent type of incidents were computer frauds. Among these, we can mention, among others, fake online stores and the financial scams popular last year, which impersonated various fuel and energy companies, firms, and institutions. The third most frequent type of incidents in 2023 was malicious software. These incidents included both ransomware infections and spam campaigns distributing Remcos and Agent Tesla software.

In addition to other destructive types of malware, ransomware currently represents a pandemic affecting both individuals and organizations worldwide, including in Poland.

An analysis of cyber incidents reported to CERT teams shows that organizations must continually adapt their security strategies to evolving threats. Key findings highlight the necessity of user education, regular updates, implementation of protective mechanisms, and having effective procedures for monitoring and responding to incidents. Through these actions, organizations can significantly reduce the risk of major cyber incidents.

5. Conclusions

Cybersecurity plays a crucial role in managing a modern organization. It protects not only sensitive data and systems but also the company's reputation and financial resources. In the era of digital transformation, cyber threats are becoming increasingly sophisticated and widespread, requiring organizations to continually adapt their security strategies. Implementing effective protective mechanisms,

educating employees, and constantly monitoring and analysing threats are the foundations of an effective cybersecurity strategy. Organizations must invest in modern protection technologies and collaborate with specialized teams, such as CERT, to ensure a quick and effective response to incidents.

Continuous research and implementation of the latest protection technologies, such as artificial intelligence (AI) and machine learning (ML), which can predict and detect new types of threats, are necessary.

Further research into the application of AI and ML in cybersecurity can significantly enhance organizations' ability to respond swiftly to threats. Human error is one of the weakest links in the security system. Regular training and increasing employee awareness are essential. Research on the most effective methods of training and educating employees should be conducted to minimize the risk of human error.

Cyber threats are constantly evolving, requiring continuous monitoring and analysis of new trends and techniques used by cybercriminals. Continuous research on new threats, including studies on specific industries and sectors, is required to create dedicated protection strategies.

Organizations differ in size and resources, meaning that protection mechanisms must be scalable and tailored to the specific needs of each company. Research on creating flexible and scalable security solutions that can be adapted to different types and sizes of organizations is crucial.

Cybersecurity is an indispensable element of managing a modern organization. Effective protection strategies must be dynamic, multi-layered, and based on the latest technologies and best practices. Further research and analysis in the field of cybersecurity are essential to ensure lasting protection against increasingly advanced threats. Only through continuous improvement and adaptation can organizations effectively protect their resources and ensure stable development in the digital era.

References:

CERT Polska. https://cert.pl/.

Levy, Y. 2015. National Institute of Standards and Technology (NIST) Cybersecurity Framework In Action! CCE Faculty Proceedings, Presentations, Speeches and Lectures. 300. https://nsuworks.nova.edu/gscis_facpres/300.

Loishyn, A., Hohoniants, S.Ya., Tkach, M., Tyszczenko, M.H., Tarasenko, N.M., Kyvliuk, W.S. 2021. Development of the Concept of Cybersecurity of the Organization, TEM Journal, nr 3.

Mąkosa, G. 2019. Zarządzanie ryzykiem jako determinanta cyberbezpieczeństwa. Nowoczesne Systemy Zarządzania, Zeszyt 14, nr 3.

Known Exploited Vulnerabilities Catalog, CISA. https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

NIST. https://nvd.nist.gov/.

Ramy Zarządzania Ryzykiem w Organizacjach i Systemach Informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu, 2021.

Ramy cyberbezpieczeństwa NIST: szczegółowy przegląd, https://www.ssl.com/pl/artyku%C5%82/szczeg%C3%B3%C5%82owe-om%C3%B3wienie-nistowych-ram-cyberbezpiecze%C5%84stwa/.

Raport roczny z działalności CERT Polska 2023. https://cert.pl/uploads/docs/Raport_CP_2023.pdf.

Roszyk-Kowalska, G., Chudziński, P. 2023. Ryzyko i zarządzanie ryzykiem w organizacjach publicznych. In: Red. A. Frączkiewicz-Wronka, M. Ćwiklickis, Zarządzanie publiczne. Perspektywa teorii i praktyki. Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice.

Szafranek, D. 2021. Wpływ rozwoju cyberprzestępczości na funkcjonowanie współczesnych organizacji. Nowoczesne Systemy Zarządzania, Zeszyt 16, nr 4, 47.

Shuliak, A., Shuliak, N. 2020. Practices for the implementation and support of the information security policy. Inskrypcje. Półrocznik, R. VIII, z. 2(15).

The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology.

Urząd Komisji Nadzoru Finansowego. https://cebrf.knf.gov.pl/encyklopedia/hasla/385-definicje/788-cert-polska.

Wojtyto, D. 2019. Metodyka zarządzania ryzykiem w organizacji. Organizacja i zarządzanie, 12/2019.

Założenia Ramowe Cyberbezpieczeństwa – Identyfikacja. https://seqred.pl/zalozenia-ramowe-cyberbezpieczenstwa-identyfikacja/.