European Research Studies Journal
Volume XXVII, Issue 1, 2024

pp. 365-379

Strategies for Effective Cybersecurity Management in Organizations

Submitted 15/01/24, 1st revision 12/02/24, 2nd revision 22/02/24, accepted 31/03/24

Marek Ciekanowski[1], Sławomir Żurawski[2], Yury Pauliuchuk[3], Zbigniew Ciekanowski[4], Stanisław Marciniak[5]

Abstract:

Purpose: *The purpose of this article is to analyse management actions aimed at increasing the level of cybersecurity within an organization.*
Design/Methodology/Approach: *The article addresses various aspects of cybersecurity, referencing statistical data related to ICT security in enterprises as well as incidents occurring in businesses both in Poland and the EU. Analysis of incident data facilitated determining the impact of cyber threats on organizational security and operations. The research problem was formulated as: How can proper cybersecurity management in an organization influence its functioning? Corresponding to the research problem, the following hypothesis was adopted: Proper cybersecurity management in an organization enhances its operational efficiency. Verification of the hypothesis and obtaining answers to the posed questions required the application of research methods. For the research, literature analysis, the examination of legal acts concerning cybersecurity, and a detailed analysis of data from national and international reports in the studied area were utilized. The authors also considered their existing knowledge in this field.*
Findings: *Cybersecurity management is a crucial element of contemporary organizational functioning. Organizations that do not take action in cybersecurity expose themselves not only to the risk of financial losses or reputation damage but even to the cessation of operations.*
Practical Implications: *Cybersecurity needs to be approached systematically. It is extremely important to engage in cooperation and utilize solutions from entities that provide us with an adequate level of cybersecurity.*
Originality/Value: *In this study, the authors presented the legal regulations of Poland and the European Union in the field of cybersecurity, described aspects of cybersecurity management, and presented the roles of cybersecurity management in the functioning of*

[1]*University of Social Sciences, Poland, ORCID: 0009-0009-1271-0652, marek@ciekanowki.pl;*
[2]*State School of Higher Education in Chełm, Poland, ORCID: 0000-0001-9527-3391, slawomir.zurawski@onet.pl;*
[3]*Siedlce University of Natural Sciences and Humanities, Poland, ORCID: 0000-0002-2077-5124, y.pauliuchuk@wp.pl;*
[4]*Faculty of Economics, John Paul II University of Applied Sciences in Biała Podlaska, Poland, ORCID: 0000-0002-0549-894X, zbigniew@ciekanowski.pl;*
[5]*Warsaw Management University, Poland, ORCID ID: 0000-0003-0406-1487, s.marciniak2@wp.pl;*

contemporary organizations. The authors also outlined principles that can help in managing cyber risk in modern enterprises.

Keywords: *Organization, cyber security, threats, management, system.*

JEL: *K24, M10, M15.*

Paper type: *Research article.*

1. Introduction

Cyberspace has become an integral part of our lives, without which it would be difficult to imagine today's world. Cyberspace has enabled us to communicate freely, exchange information, and have unlimited access to knowledge, as well as the ability to create new social bonds. Often cyberspace is equated with the Internet, but it is a much broader area that is constantly expanding.

Alongside its undeniable advantages, this continuous growth in the significance and development of cyberspace has also become a source of many serious challenges and threats to our security. The truth is that we are unaware of what information about us, or concerning us, is being transmitted, when, how, and to whom, who may have or already has access to it, and what impact the loss of confidentiality of this information may have on us.

The necessity to implement security measures to protect against cyber attacks is obvious in today's times. Ransomware attacks, data theft, or disk encryption are just some of the threats that almost every modern organization must confront nowadays. The problem affects both large and small enterprises, as well as governmental and local administrative units.

Therefore, cybersecurity needs to be approached systematically, as cooperation and utilizing solutions from entities that provide us with an adequate level of cyberspace security are extremely important in this area.

2. Legal Regulations of Cybersecurity

The aim of the national cybersecurity system is to ensure cybersecurity at a national level, which involves the uninterrupted provision of key and digital services, to be achieved by ensuring an adequate level of security in information systems used to provide these services (Act of July 5, 2018, on the National Cybersecurity System. Journal of Laws 2018, item 1560, art. 3.). In Poland, cybersecurity issues are regulated to some extent by the Act on the National Cybersecurity System.

It specifies the duties and tasks of entities within the system, which are detailed in the Act. According to the law, entities such as:

- key service operators,
- key service providers;
- sectoral cybersecurity teams,
- entities of the public finance sector,
- commercial law companies performing tasks of a public utility nature,
- entities providing cybersecurity services (Act of July 5, 2018, on the National Cybersecurity System. Journal of Laws 2018, item 1560, art. 4.).

Additionally, the law specifies a catalogue of competent authorities for cybersecurity matters. They have been assigned to entities depending on the sector of their activity (source: https://www.lex.pl/cyberbezpieczenstwo-w-przedsiebiorstwie,20440.html). Below, in Table 1, the authorities responsible for cybersecurity matters are presented with their respective assigned entities.

Table 1. *Agencies Responsible for Cybersecurity in Poland*

Sector	Responsible Entity
The Energy Sector	The Minister responsible for energy issues
The Transport sector excluding subsectors of water transport	The Minister responsible for transport issues
The subsector of water transport	The Minister responsible for maritime economy and the Minister responsible for inland navigation
The banking sector and financial market infrastructure	The Financial Supervision Commission
The Health Protection Sector	The Minister of Health or Minister of National Defence
The sector for the supply of drinking water and its distribution	The Minister competent for water economy affairs
The Digital Infrastructure Sector	The Minister responsible for digitization or The Minister of National Defence
Deliveries of digital services	The Minister competent for matters of informatization or the Minister of National Defence

Source: *Own elaboration based on the Act of July 5, 2018, on the National Cybersecurity System. Journal of Laws 2018, item 1560, article 41.*

The legislator recognizes as an operator of essential services an entity that has an organizational unit in the territory of the Republic of Poland and for which the competent authority has issued a decision recognizing it as such an operator (Annexes No. 1 to the Act of July 5, 2018, on the National Cybersecurity System, item 1560).

On the other hand, a provider of essential services is a legal person or an organizational unit without legal personality having its registered office, management, or representative with an organizational unit in the territory of the Republic of Poland, providing a digital service excluding micro- and small entrepreneurs (https://www.lex.pl/cyberbezpieczenstwo-w-przedsiebiorstwie,20440.html).

In Annex No. 1 to the Act, the legislator also indicated a list of entities that are part of the operators of essential services. These include, among others:

- the energy sector,
- the transport sector,
- the banking sector and financial markets infrastructure,
- the healthcare sector,
- the drinking water supply and distribution sector,
- the digital infrastructure sector (Attachments No. 1 to the Act of July 5, 2018, on the National Cybersecurity System, item 1560).

For today, in the legal state, there is a lack of one comprehensive act regulating the entire range of cybersecurity issues in Poland. The legislator has abused the term "ensure" concerning cybersecurity, thus trivializing the essence of potential threats that could immobilize the system. It is not always possible to ensure cybersecurity, especially during such dynamic technological progress (Karpiuk, 2021).

Many aspects related to cybersecurity in Polish enterprises remain outside regulations, and entrepreneurs must ensure effective protection against threats and attacks emanating from cyberspace and effectively protect their data and pursue an appropriate cybersecurity policy (Auzina *et al.*, 2023; Grima *et al.*, 2023).

However, cybersecurity is also regulated by quite a few acts of EU law. In June 2019, the EU Cybersecurity Act came into force. It introduced, among other things, a Union-wide certification programme and a new, stronger mandate for the EU Agency for Cybersecurity (Tyagi *et al.*, 2023) (https://www.consilium.europa.eu/pl/policies/cybersecurity/#challenges).

Certification plays a crucial role in increasing trust and security for important products and services for the digital world. Currently, in the EU, there are various ICT product security certification systems. However, without common frameworks for Union-wide important cybersecurity certificates, there is an increasing risk of fragmentation and barriers between Member States (https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework).

Meanwhile, ENISA plays a crucial internal role in providing guidelines and analysis on the implementation of cyber security strategies in all EU Member States (https://www.enisa.europa.eu/topics/national-cyber-security-strategies).

Currently, the most important legal acts adopted or planned for adoption by the EU regarding cybersecurity are:

- The Directive on Network and Information Security (NIS2), which came into effect in 2023, introduces new provisions supporting a high, common level of cybersecurity across the EU. It applies to all entities whose activities may have a significant impact on the functioning of key digital services.

- The EU Cybersecurity Act, which will come into force in 2024, establishes EU-wide frameworks for the certification of cybersecurity products, services, and ICT processes. This certification aims to ensure that digital products and services are secure and comply with EU cybersecurity standards.

- The EU Cyber Solidarity Act, currently in the development phase, aims to improve readiness, detection, and response to cybersecurity incidents in the EU.

Besides these legal acts, the EU also conducts a series of actions in the field of cybersecurity, such as the "Digital Europe" programme, which allocates 1.6 billion euros for investments in cybersecurity capabilities for the years 2021-2027, or the EU Cybersecurity Strategy, which defines the EU's goals and priorities in cybersecurity until 2030.

EU legal acts concerning cybersecurity aim to ensure a high level of digital security in the EU. They are intended to assist in preventing and detecting cyberattacks, as well as responding to them. Overall, it seems that European legal frameworks regarding cybersecurity aim to address incidents and weaknesses in cybersecurity while simultaneously enhancing the security of key sectors of the economy in the EU (Chiara, 2022).

Positive steps have already been taken in EU law towards recognizing the new right to cybersecurity. Decisive progress in this direction can be observed. However, there is still much to be done (Papakonstantinou, 2022). The progress made so far must be continued and updated. Faced with contemporary challenges, businesses must place great emphasis on ensuring that alongside their core activities, regulations in the field of cybersecurity play a significant role, as well as properly identifying associated risks.

3. Cybersecurity in the Enterprise

Cyberspace is dynamically changing year by year, becoming increasingly vast and prominent across various domains (Ciekanowski *et al.*, 2023). Weaknesses in cybersecurity are widespread, occurring within organizations and posing risks to their operations. Many organizations struggle to defend their cyberspace without

clear direction or guidelines to follow. Additionally, more and more organizations describe and identify cyberattacks as having destructive consequences for their operations in a broader perspective.

Hence, security researchers have produced numerous reports on threats and attacks on organizations (Oyelami *et al.,* 2020). In the cyber context, attacks are carried out by invisible external entities that exploit organizational vulnerabilities, both technical and human. The aim is to gain access to organizational data, most commonly resulting in financial gains or other benefits such as increased competitiveness (Searle *et al.,* 2023).

A recent study conducted by Acronis in 2021 revealed that 80% of companies experienced a cybersecurity breach in the past year, compared to 68% in the previous year. Meanwhile, 9% of companies experienced at least one cyber attack per hour, illustrating the current high level of risk (source: Acronis Cyber Readiness Report 2021).

In this context, the World Economic Forum, in collaboration with the National Association of Corporate Directors and the Internet Security Association, published the Principles for Board Governance of Cyber Risk report in 2021. This report outlines six principles that can assist boards in managing cybersecurity risk. These principles are illustrated in the diagram below.

Cyberspace is changing dynamically from year to year, in various areas becoming increasingly larger and clearer (Ciekanowski *et al.,* 2023). Weaknesses in cybersecurity are common, occurring in organizations and posing a risk to their operations. Many organizations struggle to defend their cyberspace without specific direction or guidelines to follow. Also, more and more organizations describe and identify cyberattacks as having destructive consequences for their operations in a broader perspective.

Hence, security researchers have come out with numerous reports on threats and attacks on organizations (Oyelami *et al.,* 2020). In the cyber context, attacks are carried out by invisible external entities that exploit organizational loopholes, both technical and human. The goal is to gain access to organizational data, which most often leads to financial gain or other benefits such as increased competitiveness (Searle *et al.,* 2023).

A recent study conducted by Acronis in 2021 showed that 80% of companies experienced a cybersecurity breach in the past year, compared to 68% in the previous year. Meanwhile, 9% of companies experienced at least one cyber attack per hour, illustrating the current high level of risk (https://www.acronis.com/en-eu/blog/posts/acronis-cyber-readiness-report-2021-reveals-critical-security-gaps/).

In this context, the World Economic Forum, in collaboration with the National Association of Corporate Directors and the Internet Security Association, published the Principles for Board Governance of Cyber Risk in 2021. This report describes six principles that can help boards manage cyber risk. These principles are presented in the diagram below.

Figure 1. *Principles of cyber security management in an organization*

Source:*https://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021*

One of the most important elements of managing cybersecurity in an organization is risk management. It is a process that forms the basis for managing organizations, systems, areas of business or administrative activity. In recent years, we have observed dynamic actions in this area in organization management (Mąkosa, 2019).

Risk and risk management are directly and closely related to cybersecurity (Mąkosa, 2019). Therefore, in today's digital world, organizations must realize that cybersecurity is not an optional addition or just a component of their structure's functioning, but a fundamental basis of security and necessity.

Protecting sensitive data, protecting customer trust, compliance with regulations, ensuring business continuity, protecting intellectual property, managing reputation, and reducing long-term costs are important reasons why organizations should prioritize cybersecurity. (https://www.progressive.in/blog/the-crucial-importance-of-cybersecurity-for-organizations/).

Below is a presentation of the cybersecurity model in an organization using the example of a financial industry organization.

Figure 2. *7N Cybersecurity Model*

Source: *https://www.7n.com/media/hg3fqiro/7n-executive-brief-security-in-finance.pdf*

Based on the above model, it should be noted that at the beginning of the process, it is necessary to determine the areas of risk within one's organization and develop further strategy accordingly. Also important is the effectiveness of detecting potential breaches and threats and minimizing their impacts (https://gomobi.pl/raporty/cyberbezpieczenstwo-w-organizacji-krok-po-kroku/).

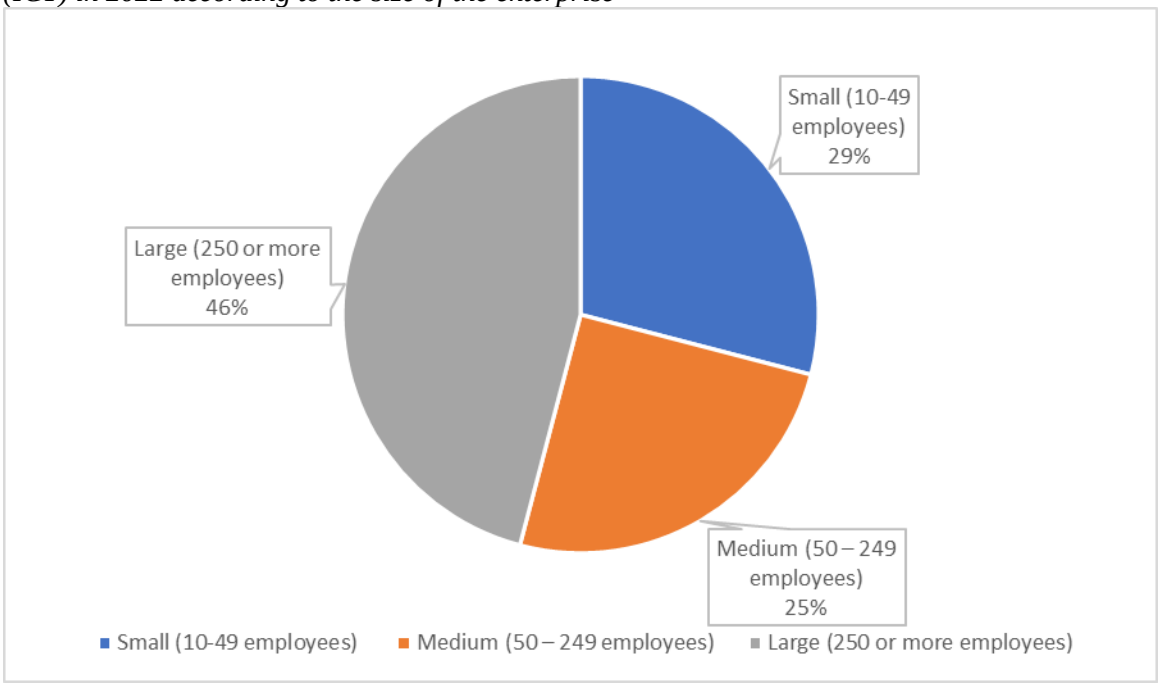
Each attempt of a cyber attack should prompt organizations to draw conclusions and implement changes in management aimed at increasing the level of cybersecurity.

4. The Role of Cybersecurity Management in the Functioning of Contemporary Organizations

Modern technologies, in order to be utilized by an organization, must be adapted to its structure, operations, and the environmental conditions in which it operates. Therefore, the utility and functionality of ICT are evolving to keep pace with dynamically occurring changes (Szota *et al.*, 2021). The recently increased activity of businesses in the digital sphere has also been driven by the crisis associated with COVID-19.

Many entities had to introduce changes in the organization of their activities (Sawicka, 2022). Chart No. 1 illustrates the equipment with information and communication technologies (ICT) in 2022 according to the size of the enterprise.

Figure 3. *Employees equipped with information and communication technologies (ICT) in 2022 according to the size of the enterprise*



Source: *Own elaboration based on: https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-komunikacyjnych-w-jednostkach-administracji-publicznej-przedsiebiorstwach-i-gospodarstwach-domowych-w-2022-roku,3,21.html*

In 2022 in Poland, the level of access to information and communication technologies (ICT) in enterprises among employees was relatively high. This was associated with benefits but also with numerous threats to the functioning of Polish enterprises and changes in their management approach. The data presented in the above chart indicate that an increasing number of employees in Poland are using ICT technologies in their work.

This is a positive trend because it can lead to increased productivity and work efficiency, facilitate communication and collaboration, and enhance employees' professional development opportunities.

However, with the increasing utilization of ICT technologies, the risk of cyberattacks also grows. Therefore, it is important for organizations to implement appropriate cybersecurity management solutions. In this context, attention should be paid to the following aspects:

Security Policy: The organization should possess a clear and transparent security policy, which defines the principles of using ICT technologies in the workplace. This policy should encompass areas such as:

a) Access to systems and data,
b) The security of devices and networks,
c) The security of personal data,
d) The security of communication.

Protection against malware: The organization should employ antivirus and anti-malware solutions to guard against malicious software.

Protection against phishing attacks: The organization should educate employees on network security, including threats associated with phishing attacks.

Response to security incidents: The organization should have a security incident response plan that defines procedures in the event of such an incident.

The implementation of appropriate solutions in the area of cybersecurity management will enable organizations to minimize the risk of cyber attacks and protect their assets. However, with regard to the EU in 2022, 92% of EU enterprises applied at least one ICT security measure to protect their ICT systems and data, while only 36% applied 7 security measures.

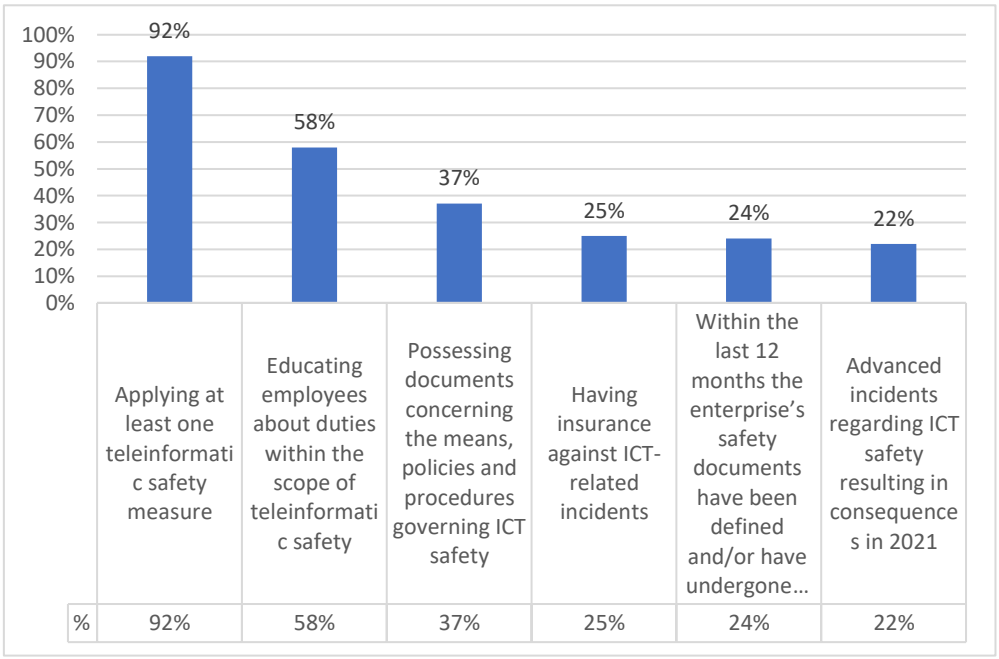
The majority of firms in the EU preferred to use strong password authentication (82% of firms in the EU), backup data creation in a separate location or cloud (78%), and network access control (65%) (source: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_in_EU_enterprises).

Figure 4 below illustrates the areas of ICT security in EU enterprises in 2022 and the percentage value of their implementation.

Data concerning the implementation of ICT security measures in the EU in 2022 indicate that the majority of enterprises in the EU are taking action to protect their ICT systems and data. This is a positive trend, as it can help minimize the risk of cyberattacks.

However, attention should be paid to the fact that only 36% of enterprises in the EU implemented 7 security measures. This means that many firms are still not taking all necessary action regarding ICT security.

Figure 4. *ICT Safety in enterprises in the EU in 2022*



Source: *Eurostat, https://ec.europa.eu/eurostat.*

Organizations should consider implementing additional security measures both in Poland and in EU countries because in 2021, more than one in five enterprises in the EU (22%) experienced ICT security-related incidents that had serious consequences, such as ICT service unavailability, data destruction or damage, or the disclosure of confidential data.

ICT security incidents may be caused by malicious attacks from external or internal sources, or by non-malicious factors such as hardware or software failures or unintentional actions by employees (Figure 10). Below are the data concerning enterprises that experienced ICT security-related incidents resulting in consequences.

The Eurostat report regarding incidents of ICT security in enterprises within the EU indicates that, in the majority of cases, damages to ICT services or enterprise data were caused by incidents that were not malicious events. The most frequently reported consequence of ICT security-related incidents was the unavailability of ICT services due to hardware or software failures (19% of enterprises).

Hardware or software failures can be caused by various factors, including cyber threats. Data suggests that enterprises should particularly focus on cybersecurity. Enterprises can minimize the risk of these incidents by implementing appropriate security measures to minimize the occurrence of ICT security incidents and protect

their assets. The role of cybersecurity management in organizational functioning can be divided into the following areas:

The protection of personal and confidential data: Personal and confidential data are valuable assets for organizations. Their loss or disclosure can have serious consequences, such as legal violations, reputation loss, or financial losses. Cybersecurity management aims to protect this data from unauthorized access, modification, or destruction.

The protection of IT systems and infrastructure: IT systems and infrastructure are essential for organizational functioning. Their failure or disruption can cause serious problems, such as a loss of data access, service interruptions, or even the need for compensation payments. Cybersecurity management aims to protect IT systems and infrastructure from attacks and other threats.

Protection against cyber attacks: Cyber attacks are becoming increasingly common and sophisticated. They can be carried out by various entities, including criminal organizations, states, and competitors. Cybersecurity management aims to prepare organizations for cyber attacks and minimize their impact.

Cybersecurity management is an ongoing process: Organizations must regularly update their security policies, identify new threats, and implement new security measures.

5. Conclusions

Contemporary organizations heavily rely on information and communication technologies (ICT). These technologies are utilized for conducting business activities, communicating with clients and employees, as well as for storing and processing personal and confidential data. With the increasing utilization of new technologies, the risk of cyberattacks also escalates.

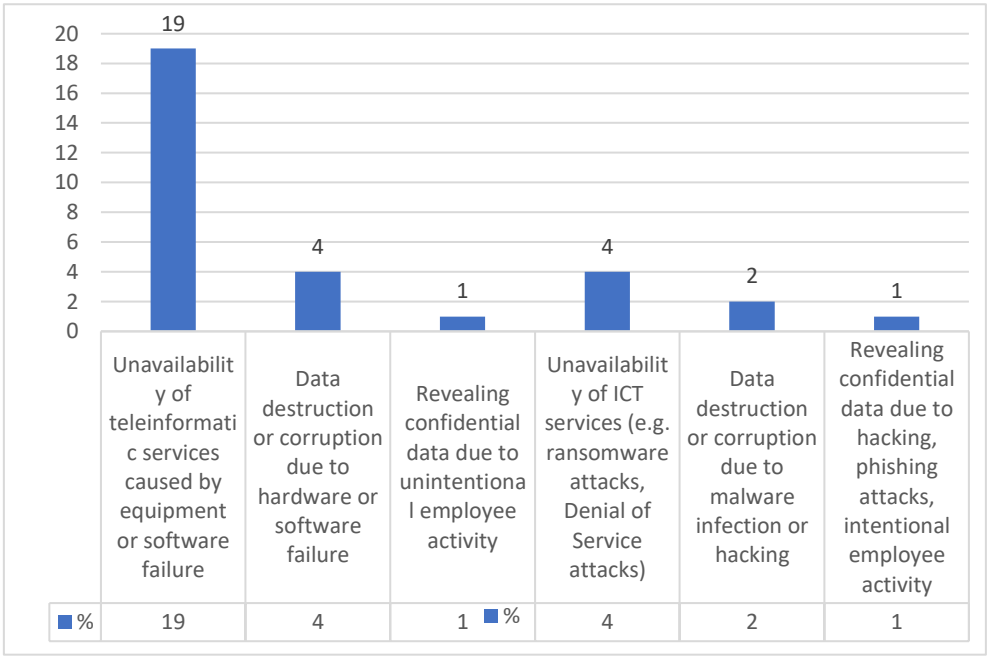
Cyberattacks can have significant consequences for organizations. To minimize the risk of cyberattacks, organizations must implement appropriate solutions in the field of cyber security management. Cyberattacks are becoming increasingly prevalent and sophisticated.

They can be carried out by various entities, including criminal organizations, states, and competitors. Cyber security management is a process that involves the identification, assessment, and control of cyber risk, aimed at preparing organizations for cyberattacks and minimizing their effects.

Cyber security management is a key element of contemporary organizational functioning. Organizations that fail to take action in the realm of cyber security

expose themselves not only to the risk of financial losses or reputation damage but also to the possibility of ceasing operations.

Figure 5. *Enterprises, which experienced incidents related to ICT security, which resulted in consequences, EU, 2021.*



Source: *Eurostat, https://ec.europa.eu/eurostat*

References:

Acronis Cyber Readiness Report 2021 reveals critical security gaps left by IT leaders. https://www.acronis.com/en-eu/blog/posts/acronis-cyber-readiness-report-2021-reveals-critical-security-gaps/.

Auzina, I., Volkova, T., Norena-Chavez, D., Kadłubek, M., Thalassinos, E. 2023. Cyber Incident Response Managerial Approaches for Enhancing Small–Medium-Size Enterprise's Cyber Maturity. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 175-190). Emerald Publishing Limited.

Bezpieczeństwo teleinformatyczne w przedsiębiorstwach – Statistics Explained (europa.eu), https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_in_EU_enterprises.

Chiara, P.G. 2022. The IoT and the new EU cybersecurity regulatory landscape. International Review of Law, Computers & Technology, Volume 36, Issue 2.

Ciekanowski, Z., Gruchelski, M., Nowicka, J., Żurawski, S., Pauliuczuk, J. 2023. Cyberspace as a Source of New Threats to the Security of the European Union. European Research Studies Journal, Volume XXVI, Issue 3, 783.

Cyberbezpieczeństwo: jak UE radzi sobie z cyberzagrożeniami. https://www.consilium.europa.eu/pl/policies/cybersecurity/#challenges.

Cyberbezpieczneństwo przedsiębiorstwo. https://www.lex.pl/cyberbezpieczenstwo-w-przedsiebiorstwie,20440.html.

Cyberbezpieczeństwo w organizacji krok po kroku. https://gomobi.pl/raporty/cyberbezpieczenstwo-w-organizacji-krok-po-kroku/.

Eurostat. https://ec.europa.eu/eurostat/.

Executive Brief Cybersecurity in the Financial Industry. https://www.7n.com/media/hg3fqiro/7n-executive-brief-security-in-finance.pdf.

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

Karpiuk, M. 2021. Organisation of the National System of Cybersecurity: Selected Issues. Studia Iuridica Lublinensia, Vol. XXX, issue 2.

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

National Cybersecurity Strategies. https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

Oyelami, J.O., Kassim, A.M. 2020. Cyber Security Defence Policies: A Proposed Guidelines for Organisations Cyber Security Practices. International Journal of Advanced Computer Science and Applications, Vol. 11, No. 8.

Papakonstantinou, V. 2022. Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? Computer Law & Security Review, Volume 44. https://www.sciencedirect.com/science/article/pii/S0267364922000012.

Principles for Board Governance of Cyber Risk. Insight Report 2021. https://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf.

Sawicka, A. 2022. Cyberbezpieczeństwo jako współczesne wyzwanie w zarządzaniu małym i średnim przedsiębiorstwem. Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie, Nr. 47.

Searle, R., Renaud, K. 2023. Trust and vulnerability in the cybersecurity context. Hawaii International Conference on System Science. Hayat Regency MAUI. https://strathprints.strath.ac.uk/82574/.

Szota, J.A., Woźniak, J. 2021. Efekty wdrażania technologii teleinformatycznych – perspektywa kształtowania bezpieczeństwa współczesnych przedsiębiorstw. Nowoczesne Systemy Zarządzania, Zeszyt 16, nr. 4.

The EU cybersecurity certification framework. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

The Crucial Importance of Cybersecurity for Organizations. https://www.progressive.in/blog/the-crucial-importance-of-cybersecurity-for-organizations/.

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

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018 poz. 1560.

Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej, przedsiębiorstwach i gospodarstwach domowych w 2022 roku, GUS. https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-

informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-komunikacyjnych-w-jednostkach-administracji-publicznej-przedsiebiorstwach-i-gospodarstwach-domowych-w-2022-roku,3,21.html.

Załączniki nr 1 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, poz. 1560.