JOURNAL OF MODERN SCIENCE
TOM 2/51/2023
www.jomswsge.com

DOI: https://doi.org/10.13166/jms/166583

Grzegorz Wojciech Pietrek
Siedlce University of Natural Sciences and Humanities, Poland
grzegorz.pietrek@uph.edu.pl
ORCID: 0000-0003-2660-8025

Klaudia Skelnik
WSB Merito University in Gdańsk, Poland
kskelnik@wsb.gda.pl
ORCID: 0000-0003-2771-3900

CYBERSECURITY AND THE SCOPE OF DESIGNING INFORMATION SECURITY SYSTEMS IN THE ORGANIZATION

CYBERBEZPIECZEŃSTWO A ZAKRES PROJEKTOWANIA SYSTEMÓW BEZPIECZEŃSTWA INFORMACJI W ORGANIZACJI

Abstract

The phenomenon known as cybercrime is gaining momentum over time, becoming an increasing threat to the security of the twenty-first century. The problem is growing and is becoming a growing challenge both for the legislator, who is required to take steps in the field of legal regulations, and for law enforcement agencies, which are expected not only to ensure security, but also to counteract the phenomenon of cybercrime. It is not the right question if, but when, a cyberattack will occur. It is necessary to be properly prepared for its early identification and proper reaction. This

reality places new demands on the organization, which is currently forced to design and operate information processing systems in secure cyberspace. The huge impact on information security organizations cannot be underestimated, every smallest decision in the organization is based on the flow of information, including in ICT systems. Taking into account the above, information was taken into account as a decisive factor determining the functioning of the organization. According to the authors, such an assumption requires describing the impact of information security management on the proper, efficient functioning of the organization in cyberspace. Increasingly, the concept of information is becoming a key category, a central point of consideration, which is a set common to research conducted at the interface of various fields and scientific disciplines. When discussing the organization of its operation and functioning, it is impossible to undertake this discussion without specifying the role of information in it, including that processed in ICT systems.

The aim of this article is to answer the research problems posed:

1. How is cybercrime shaping up in Poland?
2. What are the threats in cyberspace for organizations?
3. How do organizations counter threats in cyberspace?
4. How organizations should counter threats in cyberspace
5. How were the solutions of the EU Directive transposed into the national legal order?

The formulation of research problems made it possible to generate the main adopted goal of the research, which is to analyze the solutions adopted in organizations and their impact on cyberspace security. In addition, the issue was presented, in terms of the practical application of the applicable standards in this area.

As part of the research, the method of analyzing literature and documents relating to the studied issues and diagnostic survey was used. In addition, as part of the participatory observation, experience from participation in the implementations of the solutions described in the article was indicated and, on their basis, the following research hypothesis was formulated: Information security management determines the provision of cybersecurity in the organization, which makes it necessary to implement the applicable norms and standards in this area.

Keywords: *cybersecurity, cybercrime, cyberspace, security threat, information security, systems security*

Admission

Cybercrime as a concept has relatively quickly become a commonly used term. This is primarily due to the growing threat of this phenomenon, which is becoming more and more widespread. On the map of cybercrime, Poland has also found its place as an object and target of attacks. Therefore, the protection of cyberspace is becoming one of the key issues in the field of organizational security.

Organizations need to be aware of the need to guarantee security in cyberspace. It is an obligation, and in fact a necessity, to develop a strategy of action that will include not only combating threats, but also will allow for relatively quick elimination of risk without incurring significant losses and maintaining business continuity.

The article presents the characteristics of the phenomenon of cybercrime in Poland, indicating its most significant and important issues for the security of the organization and its information processing systems in Polish cyberspace.

Cybercrime in poland

The term *cybercrime* is rarely used in criminal legislation due to numerous terminological doubts. It is difficult to establish an unambiguous scope of meaning of this concept, because this crime evolves with technological progress. However, the creation of a definition of crime is extremely important, not only from the point of view of criminal prosecution practice or criminology, but above all it will have a direct impact on the effectiveness of the international system for combating computer crime (Kulesza, 2010, p. 149).

On the other hand, the definition formulated by Interpol is very practical and defines cybercrime in two approaches – the so-called vertical and horizontal. The vertical approach refers to crimes specific to cyberspace, i. e. those that can only be committed there, e. g. hacking, computer sabotage. On the other hand, the horizontal approach assumes the commission of crimes by means of computer techniques (e. g. computer fraud, counterfeiting of money, money laundering, etc.) (http://www.infor.pl/

prawo/prawo-karne/przestepstwa-komputerowe/298370,Czym-jest-cyberprzestepstwo.html [Accessed: 13.12.2022]).

In the Republic of Poland, cyberspace has been defined by law as a space for the processing and exchange of information, created by ICT systems (teams of cooperating IT devices and software) ensuring processing and storage, as well as sending and receiving data via telecommunications networks. more and more companies in Poland are generally aware of the risks and take care of appropriate internal regulations. However, the level of investment in security and determination to implement effective solutions is quite low. And criminals exploit it mercilessly (Article 2(1b), OJ L of 2014, item 1815, as amended).

Reports from the Internet Security Threat Report published by Symantec. According to the latest research, in 2017 Poland recorded 0.86% of all attacks on a global scale, which makes Poland ranked 26th in the world ranking considering the activities of cybercriminals. On the other hand, on the European arena, out of 46 countries, Poland ranked quite high, because it was already on the 10th place in the ranking (https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf).

The Internet Security Threat Report basically confirms the observations and analyses carried out by the CERT Polska team – namely, phishing and attacks using malware remain the most common threat (e. g. Trojans, the Mirai bot recorded in Poland in 2016).

The growing ingenuity of cybercrime is also important for the growing ingenuity of cyber perpetrators, as well as the scale of their activities, which is becoming more and more widespread.

When defining its own cybersecurity strategy, Poland carried out changes and modifications so that as a result the above concept would find its place in the Act on the National Cybersecurity System of 5 July 2018. In broad terms, this document prepares Poland for the implementation of the European Union directive in the context of jointly taken steps and measures taken to ensure a high level of security in the network and ICT systems in the territory of the Community countries. Operators of the most important and superior services will be obliged to ensure security in the network not only on their own, but also towards their customers. This sector will

include energy, transport, healthcare, banking and financial infrastructure, water suppliers and digital infrastructure (http://orka.sejm.gov.pl/proc8.nsf/ustawy/2505_u.htm).

In the simplest terms, cybercrime can be divided into two basic categories:

- crimes characteristic of cybercrime,
- crimes committed using the Internet.

The first category are crimes in which the subject of the attack is the computer itself and broadly understood data processing in IT systems.

This group includes such acts as:

- impersonating another person, fake profiles;
- unauthorized obtaining of information (hacking);
- computer eavesdropping (sniffing);
- preventing the acquisition of information;
- thwarting access to IT data;
- computer sabotage;
- distribution of malicious programs and cracking;
- the use of so-called hacking tools;
- computer fraud.

The second category includes crimes in which the computer is only a means of committing it. In this group you can mention such activities as:

- offending religious feelings (crimes against freedom of conscience and religion);
- making proposals for sexual intercourse with a minor;
- public promotion or praise of paedophilic behaviour;
- public propagation of fascist or other totalitarian state systems or incitement to hatred based on national, ethnic, racial, religious differences or because of non-denominationality (broadly understood hate speech);
- trading fictitious costs;
- disposing of one's own or someone else's identity document (crimes against the credibility of documents);
- fraud committed via the Internet, e. g. on auction sites.

Polish crime in cyberspace is characterized by the fact that these acts can mostly be classified into the second category, i. e. they are committed using the Internet.

This situation is largely due to technological progress, which is becoming easier and burdened with low costs of access to the network, launching more and more hotspots with anonymous, free Internet access or an increasing number of computers and mobile devices. Another factor is the *convenience* of those who commit such acts. The perpetrator does not have to engage as many forces and resources as in the real world. Sitting at home, with a few clicks he can commit fraud, exchange pedophilic materials, or make an entry defaming another person or offending religious feelings (Cyberprzestępczość – próba diagnozy zjawiska ekspert Wydziału Rozpoznania Biura do Walki z Cyberprzestępczością KGP Kwartalnik Policyjny 4/2017 [accessed 20.01.2023]).

However, the statistics are still alarming in 2020, a total of 10420 cybersecurity incidents were recorded, an increase of 60.7% compared to 2019. In 2020, cybercriminals very often took advantage of the circumstances caused by the COVID-19 pandemic, which transferred many of our activities to online platforms. Along with the increase in our online activity, the scale of activity of cybercriminals has also increased, who already in the first weeks of the epidemic used various types of online fraud. The targets of the attacks were both private individuals, enterprises, as well as public organizations and institutions important to the state (https://www.gov.pl/web/baza-wiedzy/raport-krajobraz-bezpieczenstwa-polskiego-internetu-w-2020-roku).

Statistics on reported incidents – the team recorded a total of 29,483 unique cybersecurity incidents. This is an increase of 182% compared to the previous year. The most common type of incident is still phishing. In 2021, 33,000 domains were added to the Dangerous Website Warning List. The most frequently observed scheme of fraud was the extortion of Facebook login credentials.As part of the #BezpiecznyPrzemysł campaign, CERT Polska works to increase the level of cybersecurity of industrial infrastructure, m.in by searching for vulnerabilities. In 2021, 5 vulnerabilities received a CVE number, including 2 with a high level of threat. There was a 13% increase in the number of ransomware incidents. Critical security vulnerabilities have been

identified in Vmware vCenter, Microsoft Exchange, and Apache Log4j. The use of three new families of Trojans for the Android platform was observed: Flubot, BlackRock and ERMAC. Due to the increasing frequency of using SMS to distribute malicious links, CERT Polska has launched a special phone number +48 799 448 084, to which you can report an incident (https://cyberpolicy.nask.pl/aktualnosci/raport-cert-polska-za-2021r/).

According to the CERT Polska report on the state of security on the Polish Internet, in 2021 the CSIRT NASK team recorded 116,071 notifications of a potential ICT incident. Of which nearly 35% turned out to be unique cybersecurity incidents (29483). According to the data from the report, both indicated numbers are very high. Compared to 2020, CERT Polska in 2021 recorded an increase in incidents handled at the level of 182%.

According to data from the CSIRT GOV report, in 2020 , as in the previous one (2019), the most incidents were classified among the following three categories: virus (16777), scanning (2604), phising (1396). Considering the distribution of incidents by sector, in 2020 the largest group were incidents related to state offices – 8,356 incidents. The data of the CERT NASK report from 2021 show different data in the context of incident types. The most common type of attack in 2021 was phishing and accounted for as much as 76.57% of all handled incidents.

The development of cyberattacks is particularly influenced by the speed of information exchange, the belief in anonymity and carelessness of users. These factors contribute to the fact that cybercrime is one of the fastest evolving criminal activities. The development of technology and the Internet has significantly improved the quality of our lives, but this does not change the fact that using the benefits of technology from year to year we have to be more and more cautious users (Cybercrime – in Poland and in the world – Thinkstat [accessed: 10.01.2023]).

Extremely important in the matter of considering the issue of cybercrime in Poland remain the provisions of law, and in fact their mismatch with the dynamic development of this field of crime. Not without significance is also the unpleasant fact related to the relatively low level of training of officers combating the phenomenon, and thus also the inadequate level of their knowledge. Problems are caused by the very act of gathering evidence in the case,

while further complications arise in relation to the low level of expertise of both judges and prosecutors. Very often they are not able to cope with the proper use of evidence in electronic form.

When analyzing the issues of cybercrime, it is worth paying attention to its cross-border and a-geographical nature. In the case of this phenomenon, there is no way to set boundaries that will allow it to be in time and space. Data transfer takes place without any borders, both national and intercontinental. In the context of the global nature of the phenomenon, legislators face a huge dilemma, who are required to unify the law to such an extent that it is possible to fight cybercrime anywhere in the world in the same way and on the same scale, while applying uniform legal provisions, while at the moment the perpetrator of a crime is subject to punishment depending on the laws of a given country. Therefore, criminals willingly choose countries for their activities where the system of legal regulations has significant loopholes and does not fully organize the issue of criminal liability of the perpetrator of a prohibited act (Siwicki, 2013, pp. 77 – 78).

In 2016, NATO recognized cyberspace as the fifth treaty area of responsibility, after land, sea, air and space. Therefore, in the present world, no organization, man, or state should feel completely safe. Many research organizations confirm that cybercriminals massively paralyze the functioning of organizations, destroy IT architecture, capture capital, hinder access to resources, modify, copy, or steal data.

Cybersecurity assumes ensuring the security in the network of digital resources, processes, and activities in information systems. The most important resources include, above all, capital, IT infrastructure and information. Currently, great emphasis is placed on cybersecurity in industries where extensive systems are used and where data about users, partners or the company are processed.

Cybersecurity of the organization – conditions and requirements

Cyberspace has become an area of activity of the organization as important as the material plane. In parallel, actions taken in material and virtual reality are treated as related and necessary areas of activity of entities. This observation affects the perception of threats in cyberspace and determines the need to analyze the existing and forecasted security threats of individuals involved in economic and social life. Cyberspace has become an area of proper activity of organizations for which information is the subject of undertaken activities, which treat information tools as an essential element of operational management and support for implemented activities at the level of control, communication, information collection.

To live and act in the modern world means to use information, and information resources as part of the optimal functioning of the organization are processed using ICT systems that operate in cyberspace. Ensuring cybersecurity should be at the top of the list of priorities for all organizations.

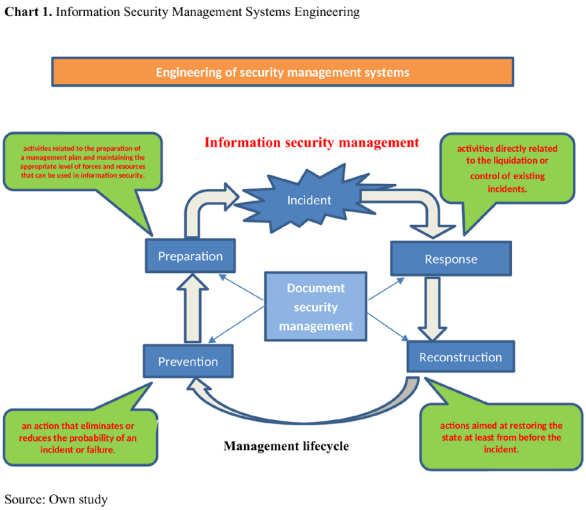
A wide range of threats related to functioning in cyberspace include disinformation, trolling, actions aimed at damaging the good name of the company or undermining its credibility, disrupting the implementation of important tasks; attacks causing disruptions to the functioning of ICT networks in organizations with a higher degree of sensitivity, including those creating critical infrastructure; the existence of technological gaps that allow to affect the ability to operate in cyberspace. The most important activities for the cybersecurity of organizations include:

- assessment of cybersecurity conditions, including identification of threats, estimation of risks and identification of opportunities;
- preventing (counteracting) threats, reducing various types of risks and taking advantage of opportunities;
- defense and protection of own systems and resources accumulated in them;
- after a possible attack, restoring the efficiency and functionality of the systems creating cyberspace (on the basis of the *Doctrine*

cybersecurity RP, wyd. BBN, Warsaw 2015, source: http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf).

As indicated by the standards in force in the field of information security and on the basis of them developed good practices, among the practical projects to ensure the effectiveness of activities in cyberspace, one can indicate, m.in, having the ability to defend and protect own ICT systems and resources accumulated in them, creating and strengthening structures intended for the implementation of tasks in cyberspace, ongoing monitoring and strengthening of network security used for distribution and storage of information and strengthening educational activities that increase the awareness of employees, members of the organization about their role in ensuring security in cyberspace. The chart below shows the engineer of the information security management system.

Chart 1. *Information Security Menagement Systems Engineering*



Source: Own study

The information age requires changes in the way we operate, but also in the way we organize – it requires the evolution of old ones or the emergence of new structures that will effectively respond to the challenges of the modern security environment. It requires security management and maintaining the continuity of operation of ICT systems. Adapting security structures to the requirements of a networked security environment is a particular challenge for an organization. The ability to function in a network-centric environment requires building organizations that achieve their goals through the flexibility of roles and activities and the speed of control processes. Such organizations, using advanced information technologies, base their activities primarily on innovative leadership structures, striving to respond as quickly as possible to emerging challenges, threats and changes in situational awareness and comply with information security standards.

The answer to these challenges should be a refined and detailed doctrine of action, based on standards and good practices developed on their basis. The concept of organizations capable of innovation and rapid change to effectively adapt to new challenges assumes that such organizations change continuously, which is conditioned by difficult conditions. Among the recommendations for shaping effective cybersecurity systems, it is therefore worth indicating the most important:

- perceiving the commitment to perform tasks in cyberspace in the same way as in other important areas ensuring the security of the organization and the company;
- preparation of a *road map* of barriers in the area of cybersecurity with a plan to eliminate these barriers, a schedule and financial forecasts;
- development and implementation of algorithms of action, defining good practices and principles of action for the cybersecurity of the organization ((on the basis of the *Doctrine cybersecurity RP*, wyd. BBN, Warsaw 2015,source: http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf).).

In fact, dependence on the network and its continuous use at almost every level of the organization's functioning has become a reality, but there is still a lot missing to really adapt the structures responsible for security to the requirements of this new environment. This is especially true for security

structures. Due to the traditional approach to organizing and attachment – also in terms of organizational culture – to rigid hierarchical structures, the evolution to the form of a flexible, networked organization may prove to be a challenge not at the technological level, but at the level of the possibility of mental and mental adaptation of both the management of the organization and its individual members.

The strategy for ensuring the security of ICT systems is to build them in a way that reduces possible problems resulting from security breaches or unwanted activity of an authorized user. This approach becomes particularly important when maintaining a large infrastructure for commercial use. The goal of security management is to minimize potential losses and enable quick and efficient identification of problems.

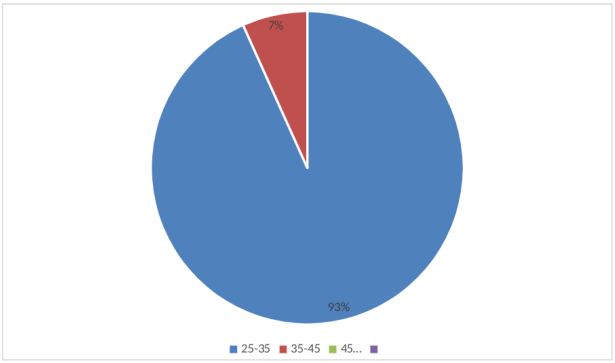
Are many standards for this process. One of the more popular and detailed examples is the two-part British standard BS 7799, Information technology – Code of practice for information security management and Information Security Management Systems – Specification with guidance for use. This standard was later adopted by ISO as ISO/IEC 17799:2003 and ISO/IEC 27001:2005. 27001:2007.

Results of own research

For the purposes of the topic of the article, a study was conducted using a survey form. The aim of the study was to check how organizations that operate in the IT sphere take care of network security in response to cyber threats. The study was conducted in 2021. It was attended by 100 respondents. The majority of respondents (93%) are aged 25-35. The remaining respondents (7%) are aged 35-45.

Figure 2 shows the percentage of three groups of respondents.

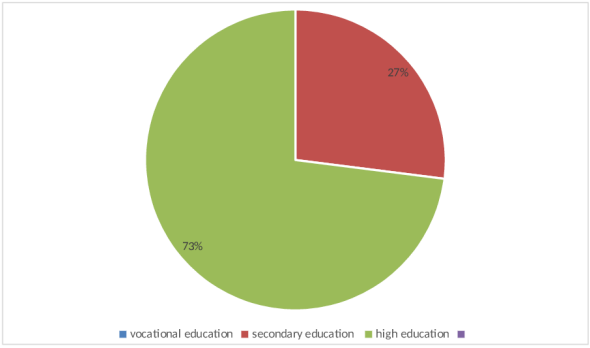
Chart 2. *Age of the subjects*



Source: Own study

The majority of respondents (73%) are people with higher education. The rest (27%) are people who have graduated from high school or technical school. The education of the subjects is illustrated in Figure 3.

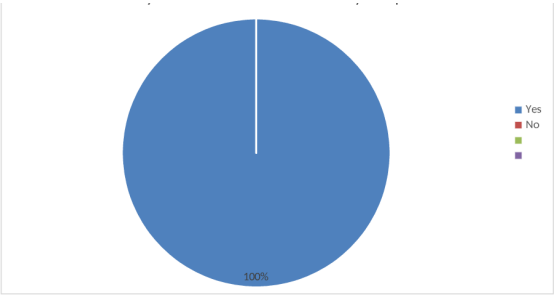
Chart 3. *Education of respondents*



Source: Own study.

In the first question, the respondents had to an`swer the question whether they are aware of the threats that occur in cyberspace. The result of the research is illustrated in Figure 4.

Chart 4. *Awareness of threats occurring in cyberspace*

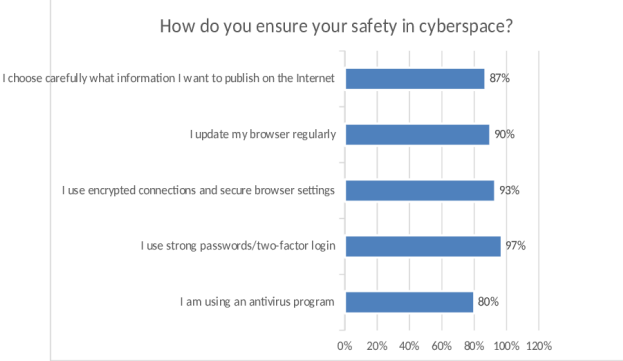


Source: Own study.

As a result of the research, information was obtained that the respondents are aware of the threats occurring in cyberspace.

The second question was a multiple-choice question. Its aim was to obtain an answer on how respondents ensure their security in cyberspace. The results of the study are shown in Figure 5.

Chart 5. *Ensuring your security in cyberspace*



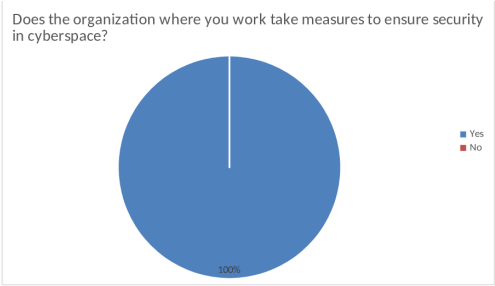
Source: Own study.

Looking at the multiple of choices, the answer turns out that 100% of employees of the companies surveyed use protection against external attacks. They differ only in the frequency of actions performed. The most common method among respondents is to use a two-level password when logging in. We also

asked about other security methods that are not shown on the chart, and these are m.in . using Linux, being up to date, scanning every downloaded file or bypassing pages of unknown origin.

In the next question, it was checked whether the organizations in which respondents work take action to ensure security in cyberspace. The results are shown in Figure 6.

Chart 6. *Taking actions to ensure security in cyberspace*

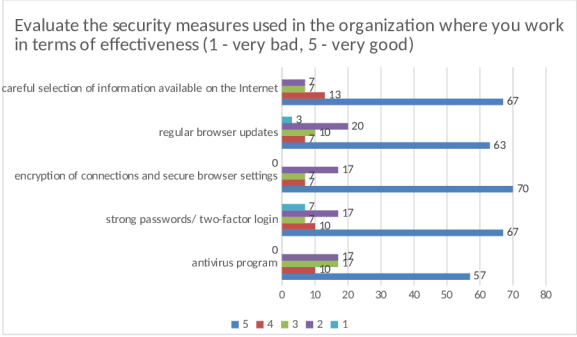


Source: Own study.

As research has shown, in each of the organizations in which the respondents work, actions are taken to ensure security in cyberspace.

The fourth question examines the security of the organization in which the respondents work in terms of their effectiveness. The results of the study are shown in Figure 7.

Chart 7. *Apply security to organizations for effectiveness*

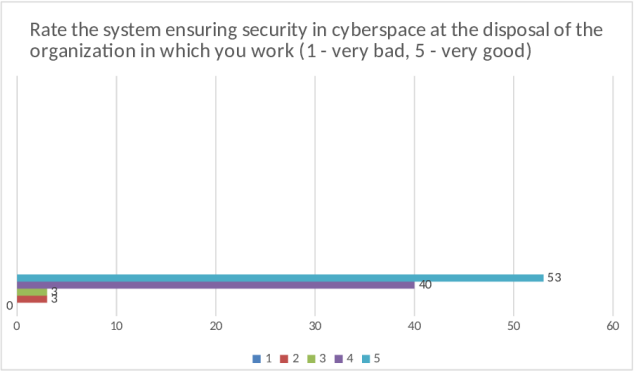


Source: Own study.

Most of the respondents rate the security in their company at a very good level. As a result of the research, it can be concluded that in organizations the worst is with the appropriate strength of the password and the selection of shared information on the network.

In the next question, respondents assessed the system of ensuring security in cyberspace that the organization in which they work has. The results of the research are shown in Figure 8.

Chart 8. *Assessment of the system ensuring security in cyberspace at the disposal of the organization*

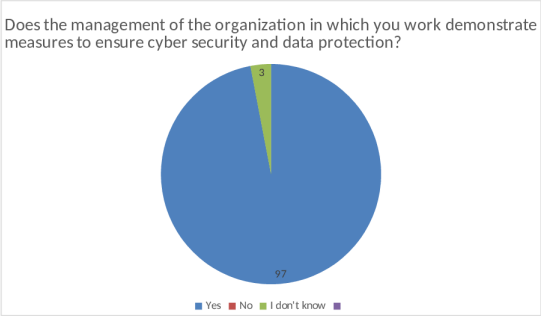


Source: Own study.

It can be said that more than 90% of interviewers are satisfied with the security system in the workplace. This is due to the positive answers obtained (read: good, very good.)

In the sixth question, respondents answered the question whether the management of the organization in which they work demonstrates activities that ensure cybersecurity and data protection. The results are shown in Figure 9.

Chart 9. *Demonstration of cybersecurity and data protection activities by the organization's management*

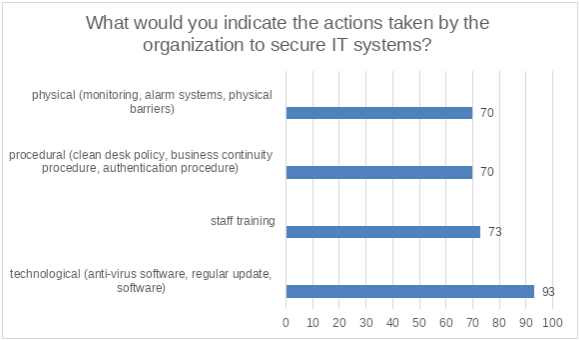


Source: Own study.

The presented results show that the majority of respondents (97%) are aware of the cyber protection activities that management provides in their workplace.

The next multiple-choice question examined what actions taken by an organization securing information systems would indicate to respondents. The results are shown in Figure 10.

Chart 10. *Actions taken by organizations securing information systems*

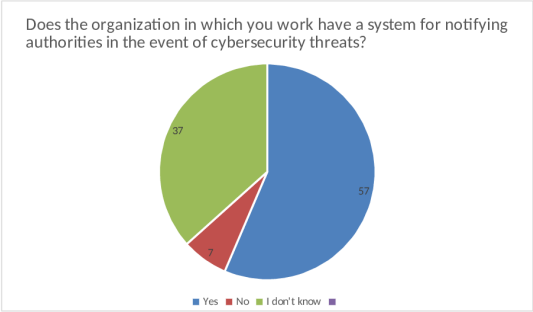


Source: Own study.

The most common it security measures among the workplaces surveyed are technological activities (93%). They were followed by employee training (73%), procedural (70%) and physical (70%) activities.

In the eighth question, respondents answered the question whether in the organization in which they work they know the system of notifying authorities in the event of cybersecurity threats. The results of the study are shown in Figure 11.

Chart 11. *Knowledge of the system for notifying authorities in the event of cybersecurity threats*

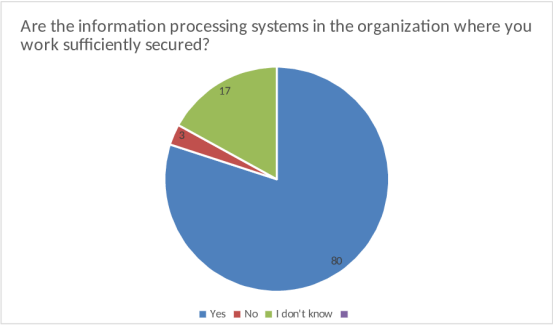


Source: Own study.

As a result of the research, information was obtained that only slightly more than 50% of people know how to behave in the event of a crime. This means that not all organizations train their employees in the event of an online emergency.

The next question concerned the security of systems processing information and data in the organization in which the respondents work. The result is shown in Chart 12.

Chart 12. *Securing systems processing information and data in organizations*

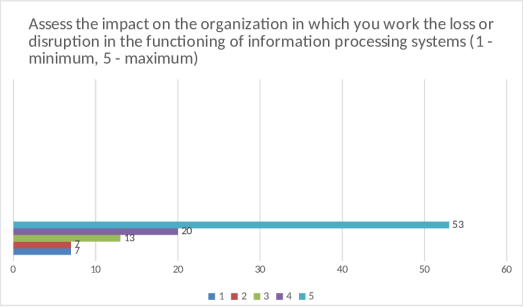


Source: Own study.

It can be considered that the majority of interviewers (80%) are satisfied with the security offered by the company where they work. Only 3% of them believe that data protection and information processing are insufficiently secured, and 17% are not sure about this.

In question 10, respondents were asked to assess the impact on organizations, loss or disruption of information processing systems. The results of the study are shown in Figure 13.

Chart 13. *Assessment of the impact on the organization of loss or disruption in the operation of information processing systems*

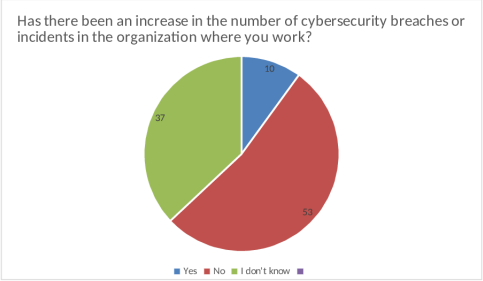


Source: Own study.

The study shows us that the loss or disruption of information processing systems has a significant impact on the work performed.

In the eleventh question, respondents answered the question whether the organization in which they work had an increase in the number of breaches or incidents related to cybersecurity. The result is shown in Figure 14.

Chart 14. *Noting an increase in the number of cybersecurity breaches or incidents in organizations*

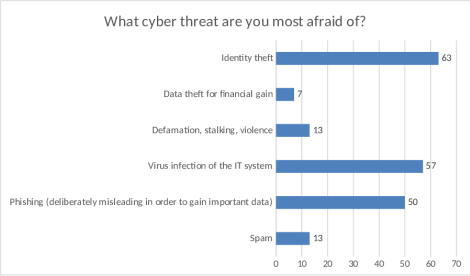


Source: Own study.

The above analysis shows that companies are eliminating cybersecurity breaches or incidents.

In the twelfth question, respondents were asked what cyber threat they fear the most, the result is shown in Figure 15.

Chart 15. *Fear of cyber threats*

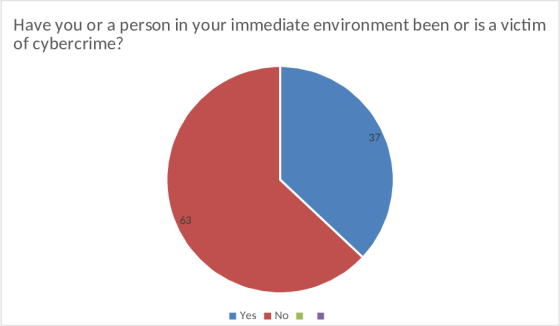


Source: Own study.

From the presented results, it can be concluded that the greatest threat to respondents is identity theft (63%). Respondents are also afraid of being infected with an IT system (57%) and phishing (50%). Astonishingly, the least of the concerns among those surveyed were defamation, stalking and violence (13%) and the threat of data theft for financial gain (7%).

In the next question, respondents answered the question of whether they or a person from their immediate environment was or is a victim of cybercrime. The results show Figure 16.

Chart 16. *The relationship with cyberbullying*

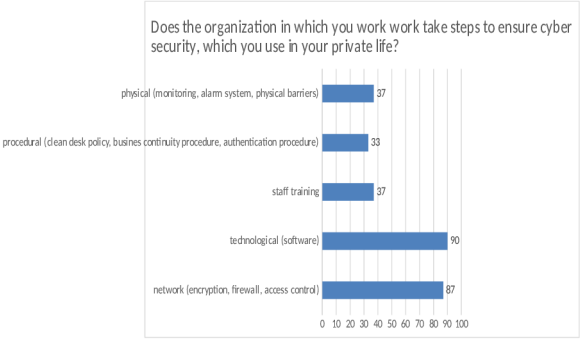


Source: Own study.

As you can see in the chart above, only 37% of the respondents had contact with cybercrime.

In the next open question, the respondents were asked to show the actions taken to ensure cybersecurity in private life. The results of the study are shown in Figure 17.

Chart 17. *Activities ensuring cybersecurity used in private life*

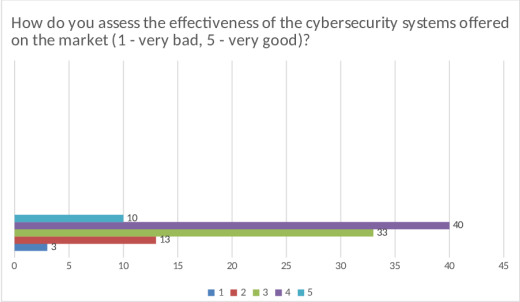


Source: Own study.

Private respondents most often choose technological security such as antivirus software or regular software updates (90%) and network security (87%). They also use the knowledge they received during trainings that took place in their workplace (37%), as well as physical security, i.e., physical barriers, monitoring, alarm systems (37%). Among the respondents, procedural safeguards were the least frequently marked answer (33%).

In the last question, the respondents were asked to assess the effectiveness of cybersecurity security systems offered on the market. The results are shown in Figure 18.

Chart 18. *The effectiveness of cybersecurity security systems offered on the market.*



Source: Own study.

The majority of respondents rate the security systems available on the market as good (40%). 10% of respondents consider them to be very good. Only 3% of them think that they are very bad. The rest of the respondents rate the systems as bad (13%) or average (33%).

The survey as a survey tool shows us that employees of the organization are well aware of the threats that occur in cyberspace. They know and are able to use various types of security to protect themselves from attacks. In their workplace, they feel safe, even though they are aware of the gaps in their security systems.

Crime prevention online

Countering cybercrime should not be based solely on the establishment of successive laws and regulations. Analyzing a wide range of crimes against digital security, the implementation of legal provisions is a kind of novelty in the criminological context. To a large extent, it penetrates into a strictly technical area in relation to the functioning of the Internet as an IT network. The reason for this state of affairs is the fact that cyber perpetrators very often use the latest technological achievements that will make it difficult or completely impossible to properly identify them. In connection with the above, with a view to eliminating criminal behavior on the Internet, it is worth noting that a much more effective tool than legal and criminal repression may be to reduce the level of risk associated with committed abuses. The foundations of security in this approach should become not only the operators providing network access services, but also the users themselves (Wójcik, 2011, p.155.).

In response to the growing demand related to the security of computer systems and the protection of information sent and processed electronically, a young scientific discipline has now been born, i.e. the security of ICT networks and computer devices. Immediately, it became an area of interest for companies, enterprises and institutions whose core business is to write computer programs, as well as to formulate security (so-called antiviruses) in relation to IT security. At the moment, it is one of the leading branches of business activity with a high level of dynamic growth.

The basic issues related to the prevention of crime in the network while maintaining the safe use of the device are primarily commonly known and used access codes and passwords. Although they are used by the vast majority of users, among others, in their e-mail boxes or when logging into a bank account, they are not sufficient protection against criminals conducting their activities on the internet. It is extremely common for Internet users not to change their passwords as often as required. At the same time, as a rule, they are not too complicated, they are an easy to bypass combination of keyboard characters. It also happens that users have the same passwords to access multiple accounts (e.g. e-mail, bank, portals and trading platforms). All this makes them an extremely easy potential target for cybercriminals.

Specialists in the field of computer law indicate that the most effective method of ensuring a high level of security in the network is the use of cryptographic methods. They allow you to protect both confidentiality (only the user who has the appropriate permissions has the ability to read the content in the right way) and authenticity (the content can only be generated by an authorized person, otherwise it will not be possible to read them correctly). This way also allows you to cover up and hide information from that group of users that does not have the appropriate permissions .

Cryptographic systems act as a kind of key (in private and public contexts) and are considered the best way to ensure network security. This is confirmed by the position of the European Commission in its communication of 8 October 1997, which indicates that the use of methods in accordance with the cryptographic key is an effective weapon in the fight against telecommunications fraud, economic espionage, piracy with regard to the protection of intellectual property, and even those crimes that are sometimes committed in connection with the unlawful use of payment cards of third parties (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0120).

Many concepts and projects are also undertaken to block or at least partially restrict access to illegal content and information placed and distributed on the internet. The filtering technology associated with the above is in fact carried out in each of the cases in a very similar way – the differences concern the planes subject to filtration and individual components in relation to which the filtering process is to take place.

An important element contributing to the protection of information systems and the information processed using them is the unfettered and autonomous nature of the content. Exceptions remain systems for the processing of personal data. The supervision of their confidentiality, integrity and availability rests with the network administrator in the context of the existence of a third party's interest in this case. This is reflected in the law and is an important element of international standards in relation to the protection of personal data.

It also happens that Polish legal regulations condition security related to integrity and confidentiality in relation to the owner of such content, who must be both the owner and user of an appropriate security system appropriate to the weight of the information. This assumption is reflected in Article 267 § 1 of

the Criminal Code. It contains a provision proving that the issue of criminal liability for a breach of information security depends on the type of breach of security that has been applied in a given case (Siwicki, 2013, pp. 83 – 84).

What is worrying, however, is a certain recklessness and lack of prudence in the face of the existence of so many measures and the constantly emerging new and innovative solutions to protect users, devices and protect against exposure to cybercrime. They shall not be used to the extent that they would minimise the risk. The awareness of a significant number of Internet users is still disproportionately low to the scope and degree of threat.

Even partial elimination of criminal activity in the network becomes possible at the moment of large-scale cooperation of both private users, as well as entities of the nature of companies, institutions, and above all law enforcement agencies and relevant services guarding the broadly understood security of the state. The active activity and synergy of the above-mentioned in pursuit of the common goal of secure cyberspace could significantly contribute to the levelling of illegal activity in the network.

However, it should also be noted that even the most uncompromising and stringent regulations will not be effective if the awareness of individual users does not grow. Not without significance here are educational activities from an early age, as well as the promotion of the idea of a safe Internet among its adult recipients. Despite the staggering speed of technological development, and consequently, the possibilities that today's world offers us can be illusory. In addition to the broad perspectives that can be gained through access to the network, one should not forget about the associated threats, which are also being modified to take increasingly sophisticated forms.

Environmental security in a purely physical context also remains an important element of secure cyberspace. Such protection of devices and equipment should ensure not only that threats related to unauthorised access to the network are addressed, but also that environmental factors that can have a significant impact on the functioning of the IT infrastructure. It should not be forgotten to properly and appropriately secure the machine park, thus eliminating attempts at unauthorized access. This category of prerequisites may also include adequate protection of devices against hazards such as power failure or electromagnetic radiation.

Devices used, for example, for data processing should be placed in such locations as to minimise as far as possible unauthorised access to them and to minimise the lack of proper supervision during their use.

Design, organization and operation of information security systems determinant of cybersecurity security

The concept of safety is used in many disciplines of modern science and has different meanings depending on the context of use. Many encyclopedic or dictionary items consider security as an antonym of a threat or refer only to particular types of security. According to the dictionary of social sciences, it is the same concept as the absence of physical danger or protection against it." This definition, due to its detail, is of little use for the purposes of this work (Gould, 1964).

A more general statement is given by the political scientist of the Polish Academy of Sciences J. Stańczyk: *security is a state of certainty, peace, security and its sense, as well as the absence of danger and protection against dangers*.58 According to the philosopher J. Świniarski, the essence of security lies in such forms of existence that ensure survival, survival and development and improvement (Stańczyk, 1996, p. 341).

Such definitions prove that security is a polysemantic concept. Polish Committee for Standardization defines information security as behavior the following information attributes:

- confidentiality – ensuring that information is available only to authorized persons,
- integrity – ensuring the accuracy and completeness of information and processing methods,
- accessibility – ensuring that authorised persons have access to information and assets whenever they need them.

Economic activity is inextricably linked to the processing of massive amounts of information. Some of them may be of strategic importance for

achieving the organization's goals, while others are less important. However, it is undeniable that information should be one of the most important resources of an organization, which requires adequate protection against a wide range of threats. Therefore, the problem of information security concerns every company, regardless of its size, form of organization, industry represented or level of development.

In defining the term 'information security', it seems necessary to refer to the standards ISO/IEC 27001:2007 and ISO/IEC 17799:2007, which use the term information security, where it is described as maintaining the confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability may be taken into account. The ISO/IEC 17799 standard refers to information security comprehensively and provides solutions that eliminate even the most frequently marginalized issues in the creation of security procedures, and local regulations of all countries use this document as a kind of reference**.**

It is already trivial to say that information security is one of the most important areas that should be secured by the management bodies of the organization. Information security is nothing more than *the defense of information, consisting in preventing and hindering the acquisition of data of the physical nature of the current and planned state of affairs and phenomena in one's own space of functioning and hindering the entropy of information to the knowledge and physical destruction of data carriers* (Kwieciński, 2010, p. 34).

The concept of information security should be explained by identifying the following risk areas: (Biłaś, 2017, p. 134):

- traditional information threats – espionage, subversive or sabotage activities (aimed at obtaining information, offensive disinformation carried out by other persons, entities, organizations);
- random threats – all kinds of natural disasters, catastrophes, accidents affecting the security of information in the organization (e.g. fire of a building in which information carriers are stored);
- technological threats – threats related to the collection, storage, processing and transmission of information in ICT networks (such as computer crimes, cyberterrorism, information warfare);

- risks resulting from insufficient organizational and structural solutions.

At every level of information security management, the main goal is to prevent its disclosure. It should be emphasized that too broad an understanding of security can hinder the flow of information in the state, enterprise, etc.

K. Liderman defines information security as a justified trust of an entity in the quality and availability of information obtained and used, therefore the concept of information security refers to an entity (human, organization) that may be at risk of losing information resources or receiving information of inadequate quality. In the opinion of K. Liderman, information security has not yet been clearly interpreted and together with the accompanying term *information security* is used in various senses, covering all forms, including verbal, exchange, storage and processing of information (Liderman, 2012, p. 67).

The complexity of contemporary information impact requires a broad, multidisciplinary approach to the author's approach in the article below presents selected information security threats. P. Bączek classifies information security threats into (Bączek, 2006, p 89):

- random hazards;
- traditional information threats;
- technological risks;
- risks relating to the civil rights of individuals or social groups.

According to a specific situation and requirements, information security is understood in different ways. However, regardless of who is involved and to what extent they are involved, all participants in the exchange of information strive to ensure that certain specific assumptions regarding its security have been met.

Among the numerous assumptions are: privacy or confidentiality, data integrity, authentication or identification, message authentication, signature, authorization, attestation, access control, certification, time stamping, certificate, receipt, approval, ownership, anonymity, non-repudiation or revocation.

Information security is also described in the literature as a condition in which the risk of threats related to the proper functioning of information resources is limited to an acceptable level (Wrzosek, 2010, p. 36).

The author emphasizes that the particular attention should be paid to the dependence of the increasein threats related to information security and their relationship with the effective functioning of the organization. Risks and threats are something we got used to when we finally realized that *progress* is not an unequivocal blessing. Any increase in the production of *goods* also means a greater production of *bads.* The results of a literature survey in the field of the theory of information society development allow us to conclude that there are many studies containing information on the positive and negative aspects of this issue. In addition, a separate problem is information security. The most important threat is the lack of balance between the development of the information society and knowledge of information security threats. Safety and its threat are inextricably linked. They are two points of our perception of social phenomena, because our sense of security depends on the size of the threat; the greater it is, the smaller the feeling of security and vice versa, the smaller the size of the threat, the greater the sense of security (Beck, 1992, p. 87).

Field research and my observations show that we can list situations that indicate that every action of any organization is to determine which information and to what extent is particularly vulnerable to loss, and even more so may be of interest to the competition. The purpose of this action is to indicate which information should be protected in particular. Therefore, you should constantly conduct the process of analyzing the information you have, indicating its value. Which indicates the need to manage information security. It should be remembered that it is not possible to contribute to the creation of barriers between a given organization and the environment, because the exchange of information takes place on the basis of feedback and thanks to this, the entities also have the opportunity to develop.

It should also be remembered that regardless of the size and scope of activities of a given organization, each of them should have a security policy, which is a set of rules related to all aspects of security. A security policy, also known as a security strategy, is also a set of principles, methods and tools for protecting and supervising information. It should include elements such as:

- information policy,
- protection of information,
- ICT system security policy,

- the rules for the protection of trade secrets,
- rules for the prevention of crime to the detriment of the organization.

Therefore, the optimal solution for ensuring security in cyberspace for organizations is the use in organizations of designing information security systems in the organization in accordance with applicable standards and good practices in this area.

Conclusion

The internet is an ideal room for manoeuvre for cybercriminals. The threat of crime is intensifying, becoming a real danger for every network user and owner of computer or mobile devices.

Illegal activity on the Internet is a huge problem, if only because of the anonymity of the people operating in it. Relatively rarely, they are afraid of detection, which gives them almost a free hand to act. The consequence of this is a new problem – it is extremely difficult to estimate potential losses, since it is not possible to accurately recognize the opponent and assess the real threat that his activity entails.

On the other hand, the relatively low self-awareness of potential victims of this type of attack in terms of safe use of the Internet is worrying. Equally often, victims do not report crimes committed online to the relevant services. This contributes to a misunderstanding of the gravity and consequences of the threat due to the significant dark number of crimes that law enforcement authorities have not been notified of. The low awareness of victims means that very often they are not even aware that they have become victims as a result of committing a cybercrime. An adequate example to confirm the above is the activity of the Weelsof virus. His scheme of operation was based on impersonating law enforcement agencies. It was used to infect individual network users in order to demand money from them for the possibility of unlocking the computer and restoring its proper functioning.

Not without significance is also the list of real costs of operations, which indicates that cybercrime is a much cheaper form of activity than its classic

variety. To commit a crime on the Internet, all you need is equipment in the form of a computer or other mobile device and an Internet connection. The main tool of the fight are viruses and computer worms.

It is also worth emphasizing that the establishment of various types of institutions and entities dedicated to the fight against cybercrime will not solve the problem of cyber threats. It is not an art only to fight them. Education and development research devoted to this matter should play a key role. It is necessary to educate not only professional staff who will recognize the threat in advance and will be able to counteract, but also to constantly deepen their knowledge so that they can always be one step ahead.

The dependencies and conclusions indicated by the authors are completely identical to the Europol IOCTA 2020 (**Internet Organised Crime Threat Assement**) report published in October 2020, showing that the ongoing pandemic has exacerbated all the problems known so far. The atmosphere of uncertainty combined with the sudden transition to remote work is being exploited by criminals in an increased way. The report also includes recommendations. Europol lists four key aspects in the fight against cybercrime, namely: Information Exchange, Prevention and Awareness, Improving the legal environment, Increasing law enforcement resources (internet_organised_crime_threat_assessment_iocta_2020.pdf (europa.eu) [Accesed: 10.01.2023]).

A key point in the field of both combating and preventing cybercrime should be conducted equally scientific and educational activities, as well as an integrated and uniform state security policy clearly defining the problem and defining the catalogue of forces and resources that can be used in the event of a threat.

To sum up, the research results obtained indicated that the article provided answers to the research questions contained in the content of individual subsections, and the research goal adopted in the dissertation was achieved. The result was to draw the final conclusion and verify the research hypothesis adopted in the dissertation, which says that information security management determines the provision of cybersecurity in the organization, which makes it necessary to imply the applicable norm and standards in this area.

It should be remembered that the place and role of information technologies in the management of the organization of the twenty-first century is

conditioned primarily by their usefulness. One of the aspects of this utility is the level of security of information resources collected and operated by various types of entities. Currently, in organizations, information technologies support a whole range of manufacturing and service processes. Their efficiency is determined by quick and reliable access to the requested information. Hence, information resources – especially shared ones – require appropriate protection mechanisms. Therefore, attention is paid to problems whose solution may determine the survival of the organization in a turbulent environment. Undoubtedly, one of them is the proper use and assurance of information security – as a key resource of modern organizations.

The above text does not exhaust the presented problem, constituting only the beginning of a comprehensive analysis of determining the Polish cyberspace by the use in organizations of designing information security systems in the organization in accordance with applicable standards and good practices in this area.

References

Bączek, P. (2006). *Information threats and the security of the Polish State*. Adam Marszałek, Toruń.
Beck, U. (1992). *Risk Society: Towards a New Modernity*. Translated by Ritter. Mark. Sage Publications, London.
Biłaś, A. (2017). *Security of information and services in a modern institution and company*. Warsaw.
Cyberprzestępczość– próba diagnozy zjawiska ekspert Wydziału Rozpoznania Biura do Walki z Cyberprzestępczością. KGP Kwartalnik Policyjny 4/2017
Gould, W., Kolb, L. (1964). *A Dictionary of the social sciences.* Free Press, London.
Kulesza, J. (2010). *International Internet Law*. Poznań.
Kwieciński, M. Information and Business Security: Selected Issues. Kraków.
Liderman, K. (2012). *Information Security*. Wydawnictwo Naukowe PWN, Warsaw.
Siwicki, M. (2013). *Cybercrime.* C. H. Beck, Warsaw.
Stańczyk, J. (1996). *Contemporary understanding of security.* ISP PAN, Warsaw.
Wójcik, W. (2011). *Cybercrime. Selected criminological and legal issues*, *Problems of Law and Administration.* 2011, No. 1.
Wrzosek, M. (2010). Information processes in the management of a hierarchical organization. AON, Warsaw.

Netography

CERT Polska Report, https://www.cert.pl/PDF/Raport_CP_2016.pdf
Doktryny cybersecurity RP", wyd. BBN, Warsaw 2015, source: http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf
https://cyberpolicy.nask.pl/aktualnosci/raport-cert-polska-za-2021r/
https://www.gov.pl/web/baza-wiedzy/raport-krajobraz-bezpieczenstwa-polskiego--internetu-w-2020-roku
http://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298370,Czym--jest-cyberprzestepstwo.html
internet_organised_crime_threat_assessment_iocta_2020.pdf (europa.eu)
National Cybersecurity System Act, http://orka.sejm.gov.pl/proc8.nsf/ustawy/2505_u.htm
Symantec Report 2011, https://www.computerworld.pl/news/Raport-Symantec-o-bezpieczenstwie-w-roku-2011-Polska-botnetowym-rajem,382574.html
Symantec Report 2017,https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf