DOI: 10.15611/2023.10.9.04

CHAPTER 4

The Idea of Organizational Resilience in the Face of Cybercrime

Dorota Walentek
Czestochowa University of Technology
e-mail: dorota.walentek@pcz.pl
ORCID: 0000-0003-2943-8359

Dorota Jelonek
Czestochowa University of Technology
e-mail: dorota.jelonek@pcz.pl
ORCID: 0000-0001-7487-5975

Quote as: Walentek, D., and Jelonek, D. (2023). The Idea of Organizational Resilience in the Face of Cybercrime. In M. Hajdas (Ed.), *Game Changers in Management* (pp. 54-71). Publishing House of Wroclaw University of Economics and Business.

Abstract: The digital transformation process, deepened by the outbreak of the COVID-19 pandemic, completely changes the current reality of the organization in global terms. Using digital solutions has a number of advantages, but it is also associated with numerous cyber threats. In the face of these threats, digital resilience has become a kind of business imperative. The aim of the article is to determine the level of knowledge of the organization's employees about cyber threats and the degree of their preparation for potential threats of this type. The study showed an insufficient level of recognition of cyber threats by employees of the organization. It was found that employees were not adequately prepared for potential threats by the employer, which consisted, among others, in the fact that training on digital threats was conducted too rarely. Many employees do not apply appropriate forms of data and document protection. The above conclusions should encourage managers to ensure a higher level of employee education on cybercrime, and thus to build a more digitally resilient organization.

Keywords: organisational resilience, cybercrime, cyber security

4.1. Introduction

Digital transformation, intensified by the outbreak of the COVID-19 pandemic, is a process that completely changes the current reality of the organization in global terms. It is a big challenge for those responsible for building a safe and resilient organization. The reason is the constant exposure of enterprises to a number of dangerous incidents lowering the

level of cybersecurity. Adware, logic bomb, BEC, likejacking, trojans, tabnabbing, phishing, spoofing, all are just some of the threats that can be faced by employees of the organization every day. And it is often on their awareness of digital dangers and attitudes that the security of the organization depends. This aspect has been touched upon rightly by Mitnick in *The Art of Deception: I have been breaking people, not slogans* (Mitnick & Simon 2003).

The aim of the article was to determine the level of knowledge of the organization's employees about cyber threats and the degree of their preparation for potential threats of this type. As a part of the research process, an attempt was made to answer the questions about the level of recognition of cyber threats by employees of the organization, whether organizations prepare employees for potential digital threats, and what are the most common methods of securing against cyber threats in organizations.

For an organization to be able to effectively counteract cyber threats, it should be resilient. Resilience in management has been studied on many levels since the beginning of the 21st century. However, in the face of ever-increasing cybercrime, the number of publications dedicated directly to the resilience of enterprises to digital threats is definitely insufficient. The number of articles describing the aspect of cybercrime from the point of view of organization management is also low. The present study will contribute to increasing knowledge about the resilience of organizations to digital threats by checking what is the level of awareness of employees in the field of cybercrime and the possibilities of protection against it. The study is also important from the point of view of managerial practice: it can provide an indication for managers whether their subordinates are prepared for preventive actions related to digital incidents threatening the organization.

4.2. The Idea of Organizational Resilience

The term *resilience* is interdisciplinary and occurs, among others, in psychology, management, or natural sciences (Masten et al., 2021, p. 524). Most often, resilience is defined as a relatively permanent property of an individual, enabling it to adapt to adversity, tragedy or threat (Rutkowska, 2015, pp. 29, 30). It is also referred to as flexibility, resilience and resilience of the individual.

Table 4.1 presents the selected definitions of resilience, referring to different scientific disciplines.

Summarizing the analysis in Table 4.1, resilience can be treated as a kind of individual trait (Acosta, 2017; Masten et al., 2021; Rutkowska, 2015; Tagde & Fredrickson, 2004) or as a process (Cicchetti, 2010; Van Breda, 2018). Regardless of the presented alternative, the key element of the definition of resilience is the individual's ability to cope with a crisis situation. In the above interpretations, the words *flexibility*, *dynamic*, *adaptation*, *threat* are repeated. Therefore, a resilient economic unit should be flexible enough to dynamically adapt to a situation that threatens its existing existence.

Table 4.1. Selected definitions of resilience

Resilience…	Authors
„…has been characterized by the ability to bounce back from negative emotional experiences and by flexible adaptation to the changing demands of stressful experiences."	Tugade & Fredrickson (2004, p. 1)
„…has been conceptualized as a dynamic developmental process encompassing the attainment of positive adaptation within the context of significant threat, severe adversity, or trauma."	Cicchetti (2010, p. 145)
„…is a relatively permanent property of an individual that enables them to adapt to adversity, tragedy, or threat."	Rutkowska (2015, p. 29)
„…can be defined as the capacity of a dynamic system, such as a community, to anticipate and adapt successfully to challenges."	Acosta et al. (2017, p. ii)
„…is the multilevel processes that systems engage in to obtain better-than-expected outcomes in the face or wake of adversity."	Van Breda (2018, p. 4)
„…it is defined for scalability and integrative purposes as the capacity of a dynamic system to adapt successfully through multisystem processes to challenges that threaten system function, survival, or development."	Masten et al. (2021, p. 521)

Source: own study based on the indicated bibliographic items.

In management, resilience is usually treated as a feature of the system and a measure of the organization's excellence, resulting from effective management in the face of a crisis. At the level of managerial competencies, resilience is interpreted as a mechanism for surviving crisis situations, a personality trait, and aggregate competency (Bugaj & Witek, 2022, p. 11).

Analysing data from the Web of Science (WoS) database, we notice that the first articles dealing with the issue of resilience were written in 1913 and referred to the elasticity of metal alloys. In turn, the publications concerning *management* and containing *resilience* among the keywords began to appear since 2000. The number of articles devoted to resilience in individual time periods is shown in Figure 4.1.

In the period from 2000 to 2009, the term *resilience* rarely appeared in the keywords of publications from the WoS database in the *Management* category: total number of publications = 54 (Figure 4.1). During this period, resilience was mainly represented by the following keywords: *management*, *performance*, *reliability*, *coordination*, *technology*, *crisis management* and *model*. Since 2010, researchers have increasingly addressed the problem of resilience in management. The number of articles falling within the *Management* category and having *resilience* among the keywords increased from 13 in 2010 to as many as 373 in 2022. A particularly large increase in the number of studies can be seen after the outbreak of the COVID-19 pandemic: 185 publications in 2002 vs. 373 publications in 2022. These figures confirm the growing need for research on the resilience of enterprises to crisis situations.

Currently, resilience in management is being studied on many levels. Figure 4.2 presents the bibliometric mapping of keywords found in the WoS database, including the term *resilience* in the *Management* category in 2020–2022.

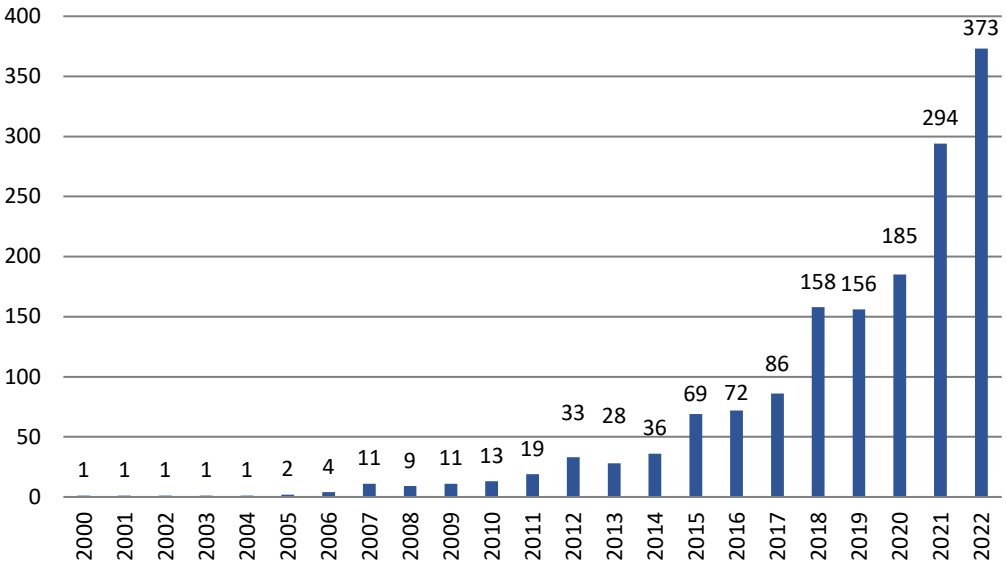

Figure 4.1. Number of publications in WoS concerning resilience and falling within the Management category

Source: own implementation based on WoS.

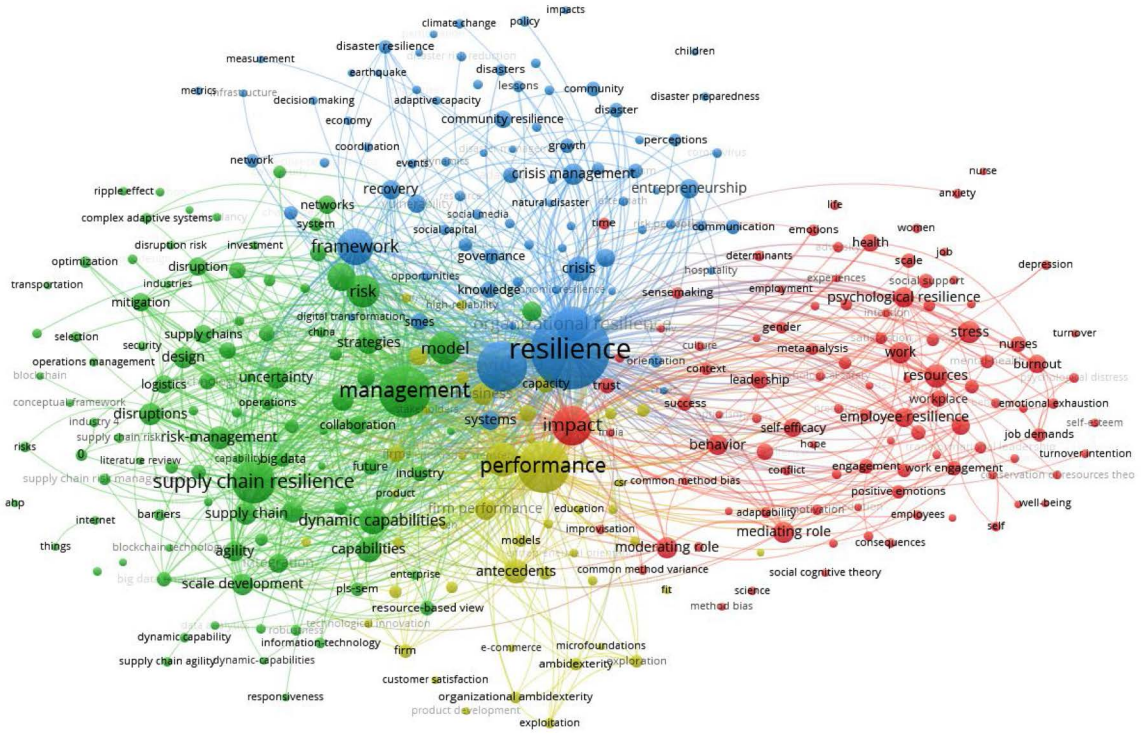

Figure 4.2. The mapping of keywords occurring in the WoS in the Management category, including the key word resilience in the years 2020–2022

Source: own implementation based on WoS.

The mapping in Figure 4.2 was performed in VOSviewer. Five was assumed as the minimum number of occurrences of the key word. A total of 326 items have been obtained, divided into four clusters. The total number of connections was 9909. For comparison, similar data for the period from 2010 to 2019 showed 218 items, five clusters and 4740 connections, and for the period from 2000 to 2009 only four items, tw clusters and 17 connections. From 2020, the term resilience most often occurs in combination with the words: *performance*, *management*, *covid-19*, *supply chain resilience*, *impact*, *framework*, *organizational resilience*, *innovation*, *risk*, *capabilities*, *risk-management*, *crisis*.

Along with the development of interest in the organization's resistance to potential threats in literature, the concept of *organizational resilience appeared*. According to DesJardine et al. (2019, p. 28), it consists in the ability of an organization to create a resilience strategy and introduce appropriate practices at the strategic, tactical and operational level in the face of subsequent crises.

Importantly, the above-mentioned crises do not have to be solely economic in nature. The role of ecological or social factors is increasingly emphasized in the literature. The crisis caused by the COVID-19 pandemic was extremely important for the increased interest in organizational resilience (Finstad, 2021; Pinzaru et al., 2020; Žítek & Klímová, 2020). Enterprises had to completely change the previously used channels of contact with the environment in a very short time. In order to stay on the market, companies have expanded their scope of activities in the digital world. And here we come to the paradox of digital transformation: the more organizations transfer their activities online, the more they are at risk of a cyberattack. Previously, the paradox of IT productivity from the perspective of managers was studied (Jelonek, 2016). However, there is no turning back from information technology, let alone from digital transformation: it is a reality to which organizations must adapt. Currently, more and more researchers describe the risks associated with digital transformation (Casey & Souvignet, 2020; Hacioglu & Sevgilioglu, 2019) and digital resilience as a necessity for organizations functioning in the 21st century (Garcia-Perez et al., 2021; Paulus et al., 2022; Tran, 2020).

4.3. Cybercrime as the Everyday Life of 21st Century Organizations

The concept of *cybercrime* has emerged with the rapid development of digital tools and the rapid spread of the Internet. The first total publications on cybercrime date back to 1995 (source: WoS database). However, the first publications in the *Management* category appeared only in 2006. Despite the ever-increasing threat of cybercrime, the list of publications until 2022 is only 78 (source: WoS, criteria: topic = cybercrime, category = *Management*).

The term "cybercrime" refers to all crimes in which the use of information technology and telecommunications networks plays an important role (Petrishcheva et al., 2019, p. 4411). A big problem of this type of crime is the fact that they are usually carried out

completely remotely and do not require as much financial outlay from the criminal as an attack in the physical world (Hui et al., 2017, p. 3). In addition, cyberattacks often remain hidden or detected with a long delay (Petrishcheva et al., 2019, p. 4411). It happens that cyber-savers illegally acquire secret data of organizations for a long time in order to sell it or achieve their own goals. These purposes may include, inter alia, increasing one's own assets by stealing company funds or destroying them.

Cybercrime can be of different scale. Some of them directly concern a person, others a specific organization, and still others – large territorial or economic areas. Countering digital attacks, especially large-scale ones, requires close international cooperation. The first international law dealing with the fight against cyberattacks was the Convention on Cybercrime developed by the Council of Europe in 2001 (Konwencja Rady Europy, 2001). However, despite the creation of international treaties, the fight against digital attacks is not easy. As emphasized by Hui and Kim (2017, p. 4), the reason for the difficult fight against cybercriminals is their very specific profile. They are often minors and are subject to significantly lower penalties than those imposed on adults. These people engage in illegal activities, believing that their knowledge and IT skills will help them avoid punishment. An additional problem may be the remote mode of digital attack and the geographical dispersion of people attempting this type of attack together. International agreements have been written about, among others, Kshetri (2013) and Hui and Kim (2017), however, even these agreements are valid in specific geographical areas, where not all members of a given group are necessarily present.

The threat of cyberattacks has increased particularly sharply during the COVID-19 pandemic. Quarantines imposed by the governments of many countries have increased the number and volume of online payments and accelerated the pace of digitalization of the economy (Afonasova et al., 2019). Thus, there is an additional space for the development of cybercrime (Kuzmenko et al., 2021). Selected digital threats are shown in Table 4.2.

The digital threats presented in Table 4.2 are divided into two types: technical and sociotechnical threats. It is an original division proposal, according to which programs and logarithms affecting data acquisition mainly at the *technical level are included in the category of technical threats*. In turn, in the category of *sociotechnical threats*, those phenomena that relate first to a specific behaviour of people are placed: their decisions, clicks, moods, etc. Cybercriminals launching an attack using a socio-technical threat count on a person's specific behaviour, e.g., clicking on a fake QR code to redirect to a fake website. It is worth noting that as a result of the user's reaction in accordance with the expectations of the criminal (in the example cited: clicking on the QR code), a technical threat may occur (e.g., downloading malware). The table also lists some of the threats that most often occur outside the structure of the organization (e.g., grooming or oversharing), but which may affect this organization by reducing the involvement of employees in the company. For example, if an employee has a ZUI team, he or she may be less effective in performing non-internet work tasks.

Due to the large number of presented threats, it was decided not to explain all the entries. Only those definitions that were used during the survey were given. These terms are

underlined and the definition is in parentheses. It is worth noting that many more digital threats are social engineering in origin. For this reason, it is crucial to constantly educate employees as individuals subject to social engineering activities about possible undesirable online activities.

Tabela 4.2. Selected cyberthreats

Technical assumptions	Sociotechnical risks	
■ adware (malware) ■ backdoor ■ information bubble ■ logic bomb (explodes suddenly after meeting certain conditions by the system/user) ■ botnet ■ browser hijacker (modification of web browser settings by a third party without the user's knowledge) ■ DDoS ■ exploit ■ fake domains ■ flooding ■ jamming ■ keylogger ■ kruegerapps ■ password spraying (the use of popular passwords by an attacker to access several accounts at the same time) ■ spyware ■ stealware	■ Business Email Compromise (impersonation of a person with whom you had business contacts) ■ clickbait (an article with a catchy title causing misinformation) ■ cybercrime ■ cyberstalking ■ digital kidnapping ■ deepfake ■ disinformation ■ doomsurfing ■ doxing ■ fake news ■ FOMO ■ flaming ■ phonoholism ■ grooming ■ happy slapping ■ hate ■ likejacking (overestimating the number of likes on social media so that the user clicks and downloads malware) ■ hate speech ■ illegal content ■ nomophobia ■ oversharing (excessive overflow in the network) ■ patocontent ■ phishing (redirecting the user to fake pages, most often via e-mail)	■ pharming (a more dangerous form of phishing; redirecting the user to fake bank websites, extorting passwords and money from them) ■ vishing (impersonation of bank employees and other trusted employees) ■ spoofing (impersonating other devices or other users) ■ phubbing ■ quishing (redirecting a user to fake pages via a QR code) ■ scam (an attempt to extort our data by promising high earnings or rewards) ■ sexting ■ sextortion ■ shareting ■ smishing (redirecting a user to fake pages via SMS) ■ making people smombies ■ tabnabbing (a form of phishing, replacing a website when a user browses another tab) ■ conspiracy theories ■ troll parenting ■ trolling ■ Internet Addiction Syndrome (IAS)

Due to the large number of presented threats, it was decided not to explain all the entries. Only those definitions that were used during the survey were given. These terms are underlined and the definition is in parentheses.

Source: own study based on OSE (2022) and Varga (2021).

The digital threats presented in Table 4.2 are divided into two types: technical and sociotechnical threats. It is an original division proposal, according to which programs and

logarithms affecting data acquisition mainly at the *technical level are included in the category of technical threats*. In turn, in the category of *sociotechnical threats*, those phenomena that relate first to a specific behaviour of people are placed: their decisions, clicks, moods, etc. Cybercriminals launching an attack using a socio-technical threat count on a person's specific behaviour, e.g., clicking on a fake QR code to redirect to a fake website. It is worth noting that as a result of the user's reaction in accordance with the expectations of the criminal (in the example cited: clicking on the QR code), a technical threat may occur (e.g., downloading malware). The table also lists some of the threats that most often occur outside the structure of the organization (e.g., grooming or oversharing), but which may affect this organization by reducing the involvement of employees in the company. For example, if an employee has a ZUI team, he or she may be less effective in performing non-internet work tasks.

Due to the large number of presented threats, it was decided not to explain all the entries. Only those definitions that were used during the survey were given. These terms are underlined and the definition is in parentheses. It is worth noting that many more digital threats are social engineering in origin. For this reason, it is crucial to constantly educate employees as individuals subject to social engineering activities about possible undesirable online activities.

From the point of view of the organization, cybercrime is a very important problem (Kshetri, 2013). Organizations should have constantly updated data and information security policies and make them known to their employees (Jelonek, 2003). The actions of digital fraudsters, including theft of funds, phishing, or deliberate destruction of IT infrastructure, can prevent business activities, lead to a decline in the reputation of the organization, and even its bankruptcy. During the research conducted by the LogRhytm institution, as many as 67% of employees confirm that their company has lost a client due to his lack of trust in the company's security strategy (LogRhytm 2022, p. 7). At the same time, the same report confirms that nearly half of companies are prepared for the growing complexity of cybercrime (48%), an increasing number of them (43%) and the evolution of threat types (42%).

An increasing number of organizations are aware of the need to protect their systems and sensitive data against cybercriminals. The main form of this type of protection is technical security, such as advanced antivirus programs, or the use of appropriate encryption programs. In enterprises, special security units are created, whose role in the proper functioning of the organization increases with the development of ICT tools and the emergence of new methods of cyberattacks. According to the report *The State of the Security Team 2022*, in 2020, only 43% of security department employees stated that they had received sufficient management support in terms of commitment, strategy and budget. In 2022, this percentage was as high as 83% (LogRhytm, 2022, p. 4).

However, even if the company spends large amounts of money to secure access to its data, it is exposed to the undesirable effects of third parties. One of the most common ways to reach the company's protected data are its employees, who do not always behave in accordance with good cybercrime practices (Abazi & Kő, 2019). This can be seen both in their work and in their private lives. According to the report *Attitudes of Poles towards*

cybersecurity (Związek Banków Polskich & Warszawski Instytut Bankowości [ZBP & WIB], 2021, p. 3), only 33% of respondents declare that they use different passwords for different electronic accounts, and 9% do not use any methods of password protection.

In order to determine the areas most exposed to cybercriminal attacks, specialists from Seon have created a ranking of countries with the highest and the weakest digital protection. According to this ranking, the best protected countries against online attacks in 2020 are Denmark, Germany, USA, Norway, Great Britain, Canada, Sweden, Australia, Japan, and the Netherlands. The least protected against cyberattacks are: Myanmar, Cambodia, Honduras, Bolivia, Mongolia, Algeria, Zimbabwe, Nicaragua, Bosnia and Herzegovina, and El Salvador (Varga, 2021). Poland was not included in the quoted list.

4.4. Research Methodology

The aim of the article was to determine the level of knowledge of the organization's employees about cyber threats and the degree of their preparation for potential threats of this type. In relation to the objective, an attempt was made to answer three research questions:

Q1: What is the level of cyber threat recognition by the organization's employees?
Q2: Are organizations preparing employees for a potential digital threat?
Q3: What are the most commonly used methods of protecting against cyber threats in organizations?

The study has been divided into two main stages: analysis of existing documents and a survey. In the first stage, the publication of *ABC Cyber Security*, created by specialists from the Scientific and Academic Computer Network – the State Research Institute (OSE IT-Szkoła, 2022), was analysed. The analysis focused on selecting the most important passwords related to cybercrime and cybersecurity in organizations. Of the nearly 100 terms found in the analysed publication, 30were selected for the next stage: 20 meaning cyber threats (including *phishing*, *oversharing*, *tabnabbing*) and 10 ways of protecting against these threats (including *updating*, *fact-checking*, *firewall*). Only passwords that may occur in the employee's professional life were selected for the study. The assessment of concepts referring mainly to the personal sphere (e.g., *troll parenting*, *grooming*) has been abandoned.

Then the second stage, i.e., the survey, was started. The questionnaire has been prepared in electronic form an was published on www.swpanel.pl and submitted for completion to registered users of the portals: www.swpanel.pl and www.ankieteo.pl. Table 4.3 summarises the questions contained in the questionnaire.

The questions collected in Table 4.3 are divided into three distinct groups. The first group consists of questions relating to the characteristics of the respondents, i.e., their gender, age and size of the company in which they work. The next group consists of introductory questions, thanks to which it was possible to determine whether the respondent uses digital technologies at work, whether he has had experience with digital threats and whether

Table 4.3. The questions included in the questionnaire

	Question	Responses
Specification	Gender:	☐ Female ☐ Male
	Age:	☐ Under 26 ☐ 26–45 ☐46–65 ☐ Over 65
	How many employees are employed by the company you work for?	☐ Less than 10 ☐ 10–49 ☐ 50–249 ☐ Over 249
Introductory	Do you use digital technologies in your work?	☐ Yes ☐ No ☐ I've never worked before
	Have you encountered any digital threats so far?	☐ Yes ☐ No ☐ I don't know ☐ I've never worked before
	Has there been a cyber-attack at the company you work for?	☐ Yes ☐ No ☐ I don't know ☐ I've never worked before
Main	Assess whether the following processes/ phenomena/tools related to the digital world threaten the security of the organization, or are they a protection against cyberattacks? In other words: are they positive or negative from the point of view of the security of the organization/company?	**Evaluation passwords:** *update*, *biometric security*, *netiquette*, *adware*, *logic bomb*, *browser hijacker*, *business e-mail compromise BEC*, *backup*, *captcha*, *cracker*, *clickbait*, *fake domains*, *malware*, *likejacking*, *oversharing*, *fact-checking*, *firewall*, *password generators*, *antivirus software*, *two-factor authentication*, *password spraying*, *pharming*, *phishing*, *vishing*, *spoofing*, *quishing*, *scam*, *smishing*, *spyware*, *tabnabbing* **Evaluation options:** 1 – *definitely a digital threat*, 2 – *rather a digital threat*, *3 – neither a threat nor a security*, 4 – *rather a protection against a digital threat*, 5 – *definitely a protection against a digital threat*, 6 – *I do not know this term*
	Think about your current employer and assess the degree to which they have prepared you for particular digital threats. If you're not currently working, think about your previous employer.	**Evaluation passwords:** *adware*, *logic bomb*, *browser hijacker*, *business e-mail compromise BEC*, *cracker*, *clickbait*, *fake domains*, *malware*, *likejacking*, *oversharing*, *password spraying*, *pharming*, *phishing*, *vishing*, *spoofing*, *quishing*, *scam*, *smishing*, *spyware*, *tabnabbing* **Responses to the choice:** *The employer has not prepared*, *The employer has prepared to a small extent*, *The employer has prepared to a sufficient extent*, *The employer has prepared very well*, *I have never worked or do not know*
	How often does your employer train you or send you cybersecurity material?	☐ Once a year or less ☐ Several times a year ☐ Several times a month ☐ I've never worked before
	What forms of protection against a digital threat and what reasons do you use?	**Evaluation passwords:** *update*, *backup*, *captcha*, *fact-checking*, *firewall*, *password generators*, *antivirus software*, *two-factor authentication*, *biometric security*, *netiquette* **Available replies:** *I do not use*, *I use – due to the requirement of the employer*, *I use – due to my own views*

Source: own work.

there has ever been a cyberattack at his workplace. The third group consists of main questions concerning the respondents' assessment of individual passwords related to cybersecurity (type A passwords) and cybercrime (type B passwords) and the process of preparing an employee by his employer to deal with a threat on the web. In question 8, all the threats that the respondents were asked about (type B passwords) were collected. In question 10, you can find a list of selected security measures/good practices for using digital devices (type A passwords). Question 7 intentionally mixes these terms. The aim was to find out the respondents' opinions on whether a given term defines a phenomenon/tool that is safe or dangerous from the point of view of an organization.

4.5. Results of the Study

The study was conducted from 09.01.2023 to 16.01.2023. The sample consisted of 239 people: 57% women and 43% men. The most numerous age group were representatives of generation Y, i.e., people from 26 to 45 years (43%). The number of other age groups was as follows: 29% of the respondents were 46 to 65 years old, 16% less than 26 years old, and 12% more than 65 years old. Most respondents worked in a microenterprise (less than 10 employees): 28%. In a small enterprise (from 10 to 49 employees) 23% of respondents were employed, in the average one (from 50 to 249 employees) – 15%, in a large (over 249 employees) – 14%. 20% had no professional experience.

In the group of people with professional experience, 60% used digital technologies in their work, 36% have personally encountered any digital threat, 41% of respondents declared that they did not have this type of experience. The answer *I don't know* was chosen by 23% of people. The respondents were also asked whether there was a cyberattack in their company. 19% answered *Yes*, 50% – *No*, and 31% – *I don't know*.

In order to answer the first research question (Q1: What is the level of recognition of cyber threats by employees of the organization?), the slogans assessed in question no. 7 were ranked in accordance with the previously assigned type: A for phenomena positively affecting the security of the organization (of a protective nature) and B for cyber threats. Then, we checked how respondents perceived individual concepts. The results have been demonstrated in Figure 4.3.

Drawing the average from individual categories, it was found that A-type passwords (of a security nature) were appropriately assigned by 35% of respondents. The correct mapping in the case of type A was considered to be answers: *rather collateral* and *definitely collateral*. The situation is much worse in the case of type B passwords (cyber threats). They were properly identified by only 18% of the respondents. *Rather, the threat* and *definitely the threat* were considered to be correct identification. This means that on average, 82% of employees of an organization either admitted that they did not know the concepts that mean cyber threats, or mistakenly described them as neutral or even positive for the security

of the organization. In view of the above, it can be concluded that the level of recognition of digital threats by employees of the organization is insufficient.

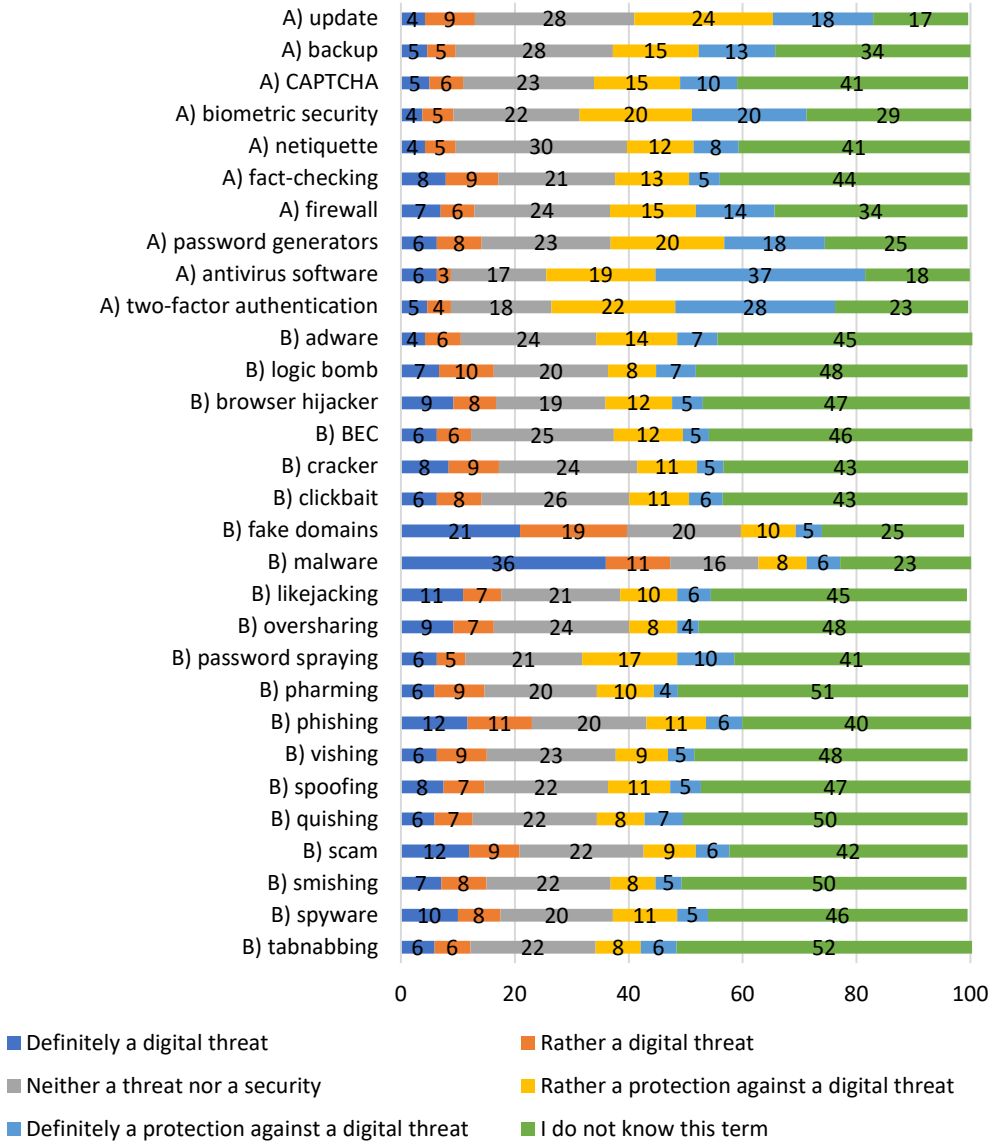

Figure 4.3. The percentage of employees assigning individual concepts to a given category

Source: own work.

It was then checked whether the accuracy of assigning threats and safeguards (or concepts that positively affect the security of an organization, such as a *netiquette*) to the appropriate category depends on the age, gender, size of the enterprise and the fact that it has faced a digital threat in the past. The χ^2 test was used. For each evaluated concept, the value of the correct mapping is given according to the evaluation description given in the case

of drawing the average. Correct mapping in the case of the accuracy of password mapping is statistically significantly ($p > 0.05$) correlated with gender in only three cases: *captcha*, *netiquette* and *fact-checking*. In these cases, men gave a much more accurate assessment. Age is correlated with the assignment of terms: *clickbait*, *fake domains*, *likejacking*, *password generators*, *antivirus software* and *scam*. The most accurate assignment can be noted among the group of people aged 26–45, then under 26, 46–65 and over 65 years of age. The size of the enterprise is statistically significantly correlated with the assignment of concepts: *backup* (the larger the enterprise, the more accurate the assignment), *antivirus software* (most accurately employees of small, then large, medium and micro enterprises) and *two-factor* credit (most accurately employees of small, then medium, large and micro enterprises). Respondents without professional experience assigned passwords the worst.

The highest number of statistically significant correlations was found between the employee's experience with the digital threat in the past and the accuracy of the assignment. In the case of the following terms: *update*, *backup*, *captcha*, *netiquette*, *likejacking*, *oversharing*, *fact-checking*, *firewall*, *two-factor authentication*, *password spraying*, *pharming*, *phishing*, *spoofing*, *scam* and *tabnabbing*, the most accurate assignment was presented by people who encountered a digital threat in the future (answer *Yes* to question No. 5), then by people giving answers *No* and *I do not know*, and the weakest people without professional experience.

Employees were also asked if their employer was preparing them for a potential digital threat (P2). The answers are presented in Figure 4.4.

The self-assessment of the degree of employee preparation for the digital threat presented in Figure 4.4 consisted in determining by the respondents whether the employer prepared them for the threat very well, to a sufficient extent, to a small extent, or did not prepare at all. The values indicated in the figure refer to the percentage of employees who assigned a given concept to a specific category. As we can see, the total percentage of respondents who admit that their organization has prepared them for a given threat to a sufficient or very good degree ranges from 36% (*BEC,tabnabbing*) to 42% (*trojan*). The average assessment of all risks was 39% (refers to the answer: *The employer prepared sufficiently* and *The employer prepared very well*). That is, far less than half of respondents say that the employer prepared them for cyber threats, which is hardly a sufficient result from the point of view of business security. The situation is further exacerbated by the fact that on average 33% of employees declare that they do not have sufficient preparation in the event of encountering a digital threat (the assessment ranges from 31% in the case of *quishing*, *phishing* and *pharming* to 36% in the case *of tabnabbing* and *BEC*).

These results are not surprising in the face of a very negative assessment of the frequency of employee training in the field of digital security. In the group of people with any professional experience, as many as 55% of respondents state that the employer trains them or submits materials with digital threats once a year or less often. The answer *A few times a year* was chosen by 25% of the respondents, *several times a month* – by 13%, and the answer *daily* was chosen by only 7%.

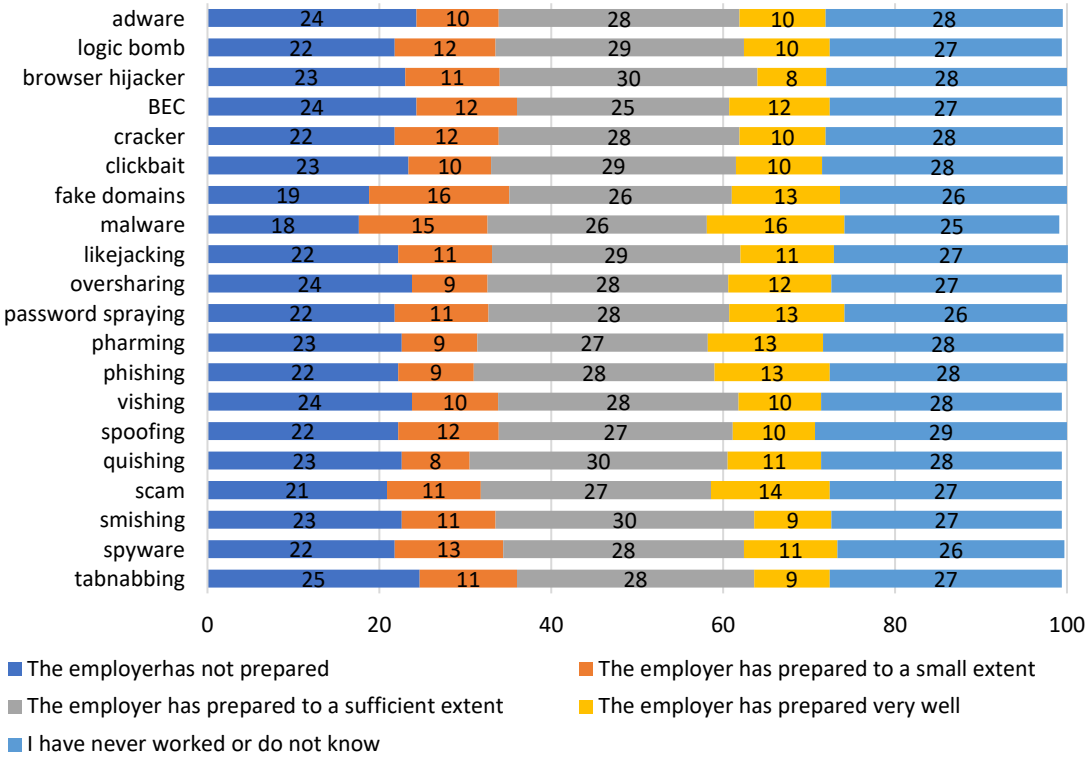

Figure 4.4. Self-assessment of the degree of employee preparation by the employer for digital threats

Source: own work.

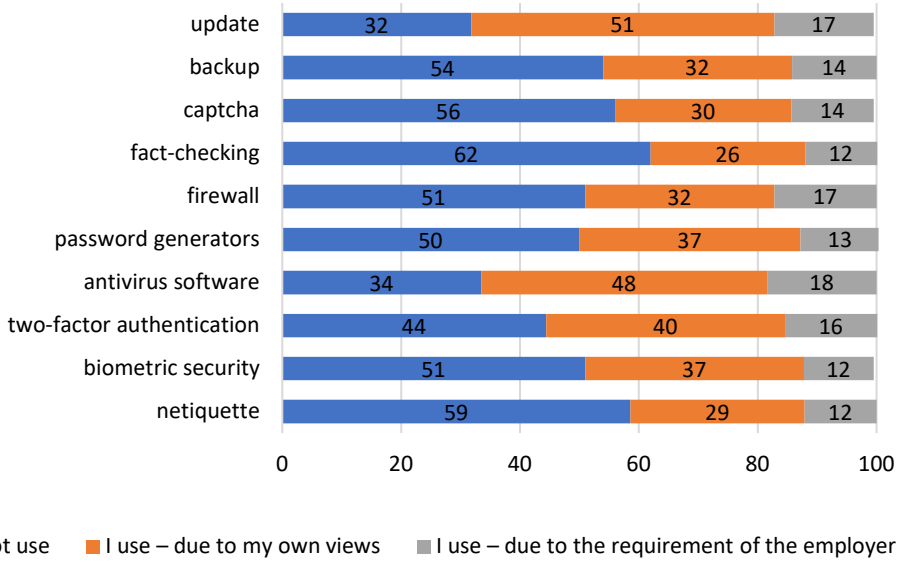

Figure 4.5. Security methods used by employees of the organization

Source: own work.

The last research area was the most commonly used methods of protection against cyber threats in organizations (P3). Employee responses in percentage terms are collected in Figure 4.5.

As shown in Figure 4.5, on average, 36% of employees use security due to their own views, and 15% due to the employer's requirement. The percentage of people not using the above forms of security ranges from 32% in the case of *updates* to as much as 62% in the case of *fact-checking*. Therefore, it can be assumed that on average 49% of employees do not use any of the analysed forms of security.

The results of the study confirm the general conclusions of the LogRhytm report (2022): at the beginning of the third decade of the 21st century companies are not prepared for threats existing in the digital environment. The conclusions of the presented study are also in line with the opinion of Abazi and Kő (2019), according to which employees are not adequately prepared for potential threats, are not able to recognize the threat and do not use sufficient forms of security. Finally: the results of this study confirm the conclusions contained in the report of the Związek Banków Polskich (Association of Polish Banks) and Warszawski Instytut Bankowości (Warsaw Institute of Banking) (2021) regarding the insufficient degree of application of safeguards against digital threats of the organization's processors.

4.6. Conclusions

Crisis situations can have a very strong impact on the structure of modern organizations. This was visible, for example, during the COVID-19 coronavirus pandemic which forced most companies to temporarily start remote work. In extreme versions, crisis situations can lead to the collapse of the organization. In order for a company to survive in times of danger, it should develop the ability to be resilient. However, it is crucial to take care of resilience before the crisis situation reveals itself. Thanks to preventive building of resilience, the organization has a chance to develop an effective immune system, especially necessary in the era of constant digital threat.

The presented research results showed an insufficient level of recognition of cyber threats by the organization's employees. The reasons for this can be found, among others, in the employer's lack of adequate preparation of employees for potential threats. Employees too rarely participate in training on how to deal with digital threats, which means that many employees do not apply appropriate forms of security.

Organizations should place greater emphasis on systematic education of employees about digital threats and methods of data and document protection. The first step may be, for example, to provide employees with more information about hazards. It is logical that the employer will not have the possibility of daily training of the employee, but every day he can send the employee, for example, an e-mail with a short information about one selected digital threat. This type of practice can significantly increase the vigilance of subordinates.

The limitation of the study is certainly the lack of division of respondents into specific industries. Cybersecurity is an important topic for every type of industry, however, it can be assumed that the level of knowledge about cybernetic threats is higher among IT industry employees than among employees from other industries.

According to the authors, further research is needed related to building organizational resilience, especially in industries that are crucial for the functioning of societies, such as the energy or medical industries. In the face of the increasing activity of cybercriminals, it is important to develop methods to prepare employees of individual organizations for attempts at cyberattacks and to educate employees in the habit of immediately responding to a potential technological threat. It is worth often and clearly emphasizing the role of digital resilience, because in the era of widespread automation of processes, it is cyber-attacks that can lead to the annihilation of an organization extremely quickly.

Organizational resilience, and in particular digital resilience, is crucial both for companies that have already started the transformation process and for those that are just starting it. In both cases, an overview of the company's practices and habits, which is the starting point for eliminating undesirable behaviours among employees and strengthening positive attitudes in terms of digital security, is extremely important to ensure the continuity of processes occurring in a given organization. Failure to take care of the preventive attitude of employees in the field of digital security may result in damage to the system by third parties, interruption of processes within the organization, and in extreme cases – the bankruptcy of the company.

Parallel to the technical security measures in place, organizations should therefore ensure continuous education of employees in the field of cyber threats. Systematic adherence to good cybersecurity practices by employees can significantly reduce or even eliminate the negative effects of digital attacks. These practices primarily concern the protection of the user's personal data, the mandatory use of up-to-date anti-virus software, setting strong passwords, logging out of transactional services after completion of activities, increased vigilance when using secured systems (e.g. electronic banking systems), not entering suspicious websites, verifying all received links, creating backup copies and habitual analysis of information read on the web in order to recognize fake news (Związek Banków Polskich [ZBP], 2022, p. 22).

References

Abazi, B., & Kő, A. (2019). Semi-automated Information Security Risk Assessment Framework for Analyzing Enterprises Security Maturity Level. In *International Conference on Research and Practical Issues of Enterprise Information Systems* (pp. 141–152). Springer. https://doi.org/10.1007/978-3-030-37632-1_13

Acosta, J. D., Chandra, A., & Madrigano, J. (2017). An Agenda to Advance Integrative Resilience Research and Practice: Key Themes from a Resilience Roundtable. *Rand Health Quarterly*, *7*(1), 1–61.

Afonasova, M. A., Panfilova, E. E., Galichkina, M. A., & Ślusarczyk, B. (2019). Digitalization in Economy and Innovation: The Effect on Social and Economic Processes. *Polish Journal of Management Studies*, *19*(2), 22–32. https://doi.org/10.17512/pjms.2019.19.2.02

Bugaj, J., & Witek, A. (2022). Rezyliencja jako element modelu kompetencji menedżera do zarządzania kryzysem. *Studia i Prace Kolegium Zarządzania i Finansów*, (184), 9–19. https://doi.org/10.33119/SIP.2022.184.1

Casey, E., & Souvignet, T. R. (2020). Digital Transformation Risk Management in Forensic Science Laboratories. *Forensic Science International*, *316*(2), 110486. https://doi.org/10.1016/j.forsciint.2020.110486

Cicchetti, D. (2010). Resilience under Conditions of Extreme Stress: A Multilevel Perspective. *World Psychiatry*, *9*(3), 145–154.

DesJardine, M., Bansal, P., & Yang, Y. (2019). Bouncing Back: Building Resilience Through Social and Environmental Practices in the Context of the 2008 Global Financial Crisis. *Journal of Management*, *45*(4), 1434–1460. https://doi.org/10.1177/0149206317708854

Finstad, G. L., Giorgi, G., Lulli, L. G., Pandolfi, C., Foti, G., León-Perez, J. M., Cantero Sanchez, F. J., & Mucci, N. (2021). Resilience, Coping Strategies and Posttraumatic Growth in the Workplace Following COVID-19: A Narrative Review on the Positive Aspects of Trauma. *International Journal of Environmental Research and Public Health*, *18*(18), 9453. https://doi.org/10.3390/ijerph18189453

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2021). Dimensions of Cybersecurity Performance and Crisis Response in Critical Infrastructure Organisations: An Intellectual Capital Perspective. *Journal of Intellectual Capital*, *24*(2), https://doi.org/10.1108/JIC-06-2021-0166

Hacioglu, U., & Sevgilioglu, G. (2019). The Evolving Role of Automated Systems and Its Cyber-security Issue for Global Business Operations in Industry 4.0. *International Journal of Business Ecosystem & Strategy* (2687––2293), *1*(1), 01-11. https://doi.org/10.36096/ijbes.v1i1.105

Hui, K. L., Kim, S. H., & Wang, Q. H. (2017). Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. *Mis Quarterly*, *41*(2), 497–523. https://doi.org/10.25300/MISQ/2017/41.2.08

Jelonek, D. (2003). Wybrane aspekty polityki bezpieczeństwa informacji w e-przedsiębiorstwie. In J. Grabara, J. Nowak (Eds.), *Systemy informatyczne. Zastosowania i wdrożenia*, Vol. III (pp. 249–256). WNT.

Jelonek, D. (2016). Paradoks produktywności technologii informacyjnych z perspektywy menedżerów. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, (421), 205–215.

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. 2015, poz. 728). https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20150000728

Kshetri, N. (2013). Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations. *Electronic Commerce Research*, *13*(1), 41–69.

Kuzmenko, O. V., Kubálek, J., Bozhenko, V. V., Kushnerov, O. S., & Vida, I. (2021). An Approach to Managing Innovation to Protect Financial Sector Against Cybercrime. *Polish Journal of Management Studies*, *24*(2), 276–291. https://doi.org/10.17512/pjms.2021.24.2.17

LogRhytm. (2022). *The State of the Security Team 2022*. https://logrhythm.com/the-state-of-the-security-team/

Masten, A. S., Lucke, C. M., Nelson, K. M., & Stallworthy, I. C. (2021). Resilience in Development and Psychopathology: Multisystem Perspectives. *Annual Review of Clinical Psychology*, *17*, 521–549.

Mitnick, K., & Simon, W. (2003). *Sztuka podstępu. Łamałem ludzi, nie hasła*, Helion.

OSE IT-Szkoła. (2022). *ABC cyberbezpieczeństwa*. https://it-szkola.edu.pl/publikacje,plik,90

Paulus, D., Fathi, R., Fiedrich, F., de Walle, B. V., & Comes, T. (2022). On the Interplay of Data and Cognitive Bias in Crisis Information Management. *Information Systems Frontiers*, 1–25, https://doi.org/10.1007/s10796-022-10241-0

Petrishcheva, N., Baybarin, A., Grebenkov, A., & Sinyaeva, M. (2019). Dark Figure of Cybercrime: Bringing It into the Light. In Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: *Education Excellence and Innovation Management through Vision 2020*, pp. 4411–4418.

Pinzaru, F., Zbuchea, A., & Anghel, L. (2020). The Impact of the COVID-19 Pandemic on Business. A Preliminary Overview. In *Strategica. Preparing for Tomorrow, Today* (pp. 721–730).

Rutkowska, M. (2015). Rezyliencja jako interdyscyplinarna kategoria analityczna i jej zastosowanie w pedagogice. *Studia i Badania Naukowe*, *9*(1), 29–47.

Tran, T., Ho, M. T., Pham, T. H., Nguyen, M. H., Nguyen, K. L. P., Vuong, T. T., ... & Vuong, Q. H. (2020). How Digital Natives Learn and Thrive in the Digital Age: Evidence from an Emerging Economy. *Sustainability, 12(9),* 3819, https://doi:10.3390/su12093819

Tugade, M. M., & Fredrickson, B. L. (2004). Resilient Individuals Use Positive Emotions to Bounce Back from Negative Emotional Experiences. *Journal of Personality and Social Psychology*, *86*(2), 320–333. https://doi.org/10.1037/0022-3514.86.2.320

Van Breda, A. D. (2018). A Critical Review of Resilience Theory and Its Relevance for Social Work. *Social Work*, *54*(1), 1–18. https://doi.org/10.15270/54-1-611

Varga, G. (2021). *Global Cybercrime Report: Which Countries Are Most at Risk?* https://seon.io/resources/global-cybercrime-report/

Związek Banków Polskich [ZBP]. (2022). *Raport cyberbezpieczny portfel 2022*. https://zbp.pl/aktualnosci/wydarzenia/Raport-Cyberbezpieczny-Portfel-2022

Związek Banków Polskich & Warszawski Instytut Bankowości [ZBP & WIB]. (2021). *Badanie „Postawy Polaków wobec cyberbezpieczeństwa"*. https://zbp.pl/getmedia/65f267e4-3316-4198-9cce-411d8f03de32/Postawy_Polakow_wobec_Cyberbezpieczenst

Žítek, V., & Klímová, V. (2020). Regional Resilience Redefinition: Postpandemic Challenge. *Scientific Papers of the University of Pardubice. Series D. Faculty of Economics and Administration*, *28*(4).

Idea rezyliencji organizacyjnej w obliczu cyberprzestępczości

Streszczenie: Proces cyfrowej transformacji, pogłębiony wybuchem pandemii COVID-19, całkowicie zmienia dotychczasową rzeczywistość organizacji w ujęciu globalnym. Korzystanie z rozwiązań cyfrowych ma wiele zalet, ale wiąże się także z licznymi cyberzagrożeniami. W obliczu tych zagrożeń swoistym imperatywem biznesowym stała się cyfrowa rezyliencja. Celem rozdziału było określenie poziomu wiedzy pracowników organizacji na temat cyberzagrożeń oraz stopnia ich przygotowania na potencjalne zagrożenia tego typu. Badanie wykazało niewystarczający poziom rozpoznawalności cyberzagrożeń przez pracowników organizacji. Stwierdzono brak odpowiedniego przygotowania pracowników na potencjalne zagrożenia przez pracodawcę, polegający m.in. na zbyt rzadkim przeprowadzaniu szkoleń z zakresu zagrożeń cyfrowych. Wielu pracowników nie stosuje odpowiednich form zabezpieczeń. Wnioski te powinny skłonić menedżerów do zadbania o wyższy poziom edukacji pracowników w kwestii cyberprzestępczości, a tym samym do budowania bardziej rezylientnej cyfrowo organizacji.

Słowa kluczowe: rezyliencja organizacyjna, cyberprzemoc, cyberbezpieczeństwo