Humanities and Social Sciences **2023**
Research Journal 30, No. 4 (2023) – part I, pp 279-293 **October-December**

Received: June 2023
Accepted: December 2023
DOI: 10.7862/rz.2023.hss.58

Dariusz TWORZYDŁO[1]
Norbert ŻYCZYŃSKI[2]
Cecília OLEXOVÁ[3]
Przemysław SZUBA[4]

THREATS FROM THE WEB AND CYBERSECURITY ISSUES FROM THE PERSPECTIVE OF PUBLIC RELATIONS PROFESSIONALS

This article aims to evaluate the approach of the public relations (PR) industry to cybersecurity-related topics. The article is based on research results conducted by a team under the authors' supervision. In 2022, we conducted quantitative research using the Computer-Assisted Web Interviewing technique (CAWI), and its purpose was to acquire knowledge in the field of perception and understanding of the cybersecurity topic by specialists in the public relations industry in Poland. The research results revealed several previously unexplored areas, highlighting gaps in current understanding. This research contributes new insights into the cybersecurity perceptions of PR professionals, enriching the existing body of scientific knowledge.

Keywords: cybersecurity, public relations, communication management, ChatGPT.

1. CYBERSECURITY. PROBLEMS AND CHALLENGES

As business and personal activities move online and the number of devices connected to the Internet and data stored and shared electronically grows exponentially, cybersecurity is becoming increasingly important, and protection against cyber threats is becoming an essential problem (Mijwil, Aljanabi, Hussein, 2023). For these and other reasons, the topic of cybersecurity is often discussed and raised in various areas of socioeconomic life. The dangers coming from the Web make it necessary not only to increase knowledge in this area, but also to constantly monitor the environment. This applies not only to individuals whose data are at risk, but also to companies. For criminals who undertake data theft, it is

[1] Dariusz Tworzydło, University of Warsaw, Poland; e-mail: dariusz@tworzydlo.pl. ORCID: 0000--0001-6396-6927.
[2] Norbert Życzyński, Rzeszow University of Technology, Poland; e-mail: n.zyczynski@prz.edu.pl (corresponding author). ORCID: 0000-0003-0681-3072.
[3] Cecília Olexová, University of Economics in Bratislava, Tajovského 13, 041 30 Košice, Slovak Republic; e-mail: cecilia.olexova@euba.sk. ORCID: 0000-0003-2154-9564.
[4] Przemyslaw Szuba, WSB Merito University in Wroclaw, Poland; e-mail: przemyslaw. szuba@opole.merito.pl, ORCID: 0000-0002-7533-7818.

clear that nowadays the value lies not only in company data, but also in the information stored on servers or computer disks. Not just bank access data anymore, but confidential information in particular is their area of interest. The mere fact of obtaining such content can be the basis, for example, for an attempt to extort a ransom under the threat of publishing the data on the TOR (The Onion Router) network. From the criminals' perspective, it is therefore an easier form of access to funds, which the victims often decide to pay to regain control over lost data. Companies that conduct cyberattacks are becoming more proficient and effective in avoiding detection. They have increasingly effective tools based on encryption using strong algorithms and advanced tactics, such as using legitimate Internet services to hide their actions and weaken existing cybersecurity techniques (Janczewski, 2022).

Safety can be defined as the objective state of not being threatened, which is subjectively perceived by individuals and groups. Therefore, security consists of two elements, objective and subjective. The first is external to the individual, the social group, and the collective. The second is subjective and concerns the feeling of being safe (Korzeniowska, 2004). Li (Li, 2011) presented the study on information privacy, referring to the competency to control information and the role of organisations, industries, and government in protecting online information and privacy of clients. Security is an expected state, while its absence causes discomfort and is a component of threat, which affects the functioning of both individuals and societies. Cybersecurity concerns the increasing possibilities of IS in collecting and using personal information of people without their knowledge (Hu, Wang, Chih, Yang 2018). Even collecting data for marketing or advertising purposes is often viewed as an action bordering on the 'almost criminal', as it undermines the autonomy of users and raises concerns about privacy intrusion (Nguyen, 2023). A threat violates the expected positive state (Kaczmarczyk, Dobrowolski, Dąbrowska, 2018). Cybersecurity is a specific type of response to threats coming from cyberspace (Chałubińska-Jentkiewicz, 2019) and it can be defined as the organisation and collection of resources, processes, and structures that are used for the protection of cyberspace and cyberspace-enabled systems from events that de jure noncompliance with de facto property rights (Craigen, Diakun-Thibault, Purse, 2014). Covers areas related to information and data sets that are only accessible to certain groups in a limited manner. Therefore, cybersecurity involves the resources, processes and structures used to protect cyberspace and the systems that support it from incidents that violate proprietary rights (Craigen et al., 2014). Cover a wide range of technical, organisational, and managerial issues that need to be considered to protect networked information systems from accidental and intentional threats (Veale, Brown, 2020). When defining cybersecurity, it is essential to take into account the supporting concepts of information security and cybercrime (Chałubińska-Jentkiewicz, 2019). The first of these concepts refers to the protection of information data first and the carriers of such data such as computers or external drives second. On the contrary, cybercrime is defined as unlawful acts undertaken with the intent to cause harm by using a computer or accessing ICT networks and it can have different forms within virtual, hybrid, or offline operations using Internet technology and cyberspace (Radhi, Hussien, Mohialden, 2023). Cybercrime manifests itself through illicit data theft, online vandalism, extortion, and various criminal endeavours seeking financial gain through coercion or deception (Nguyen, 2023).The threat of cyber-attacks is all the greater because technology changes rapidly and can be difficult to predict. The current problem is the ever-increasing sophistication of cyber-attacks. Attackers use advanced technologies, such as social engineering, malware, zero-day attacks (Ahmad, Alsmadi, Alhamdani,

Tawalbeh, 2023), which allow bypassing traditional security defences (Aji, Widod, Aji, Aji, Prawitasari, 2023). In addition, this complexity is increased by the interconnection of digital systems and the rapid adaptation of new technologies such as cloud computing and the Internet of Things (IoT). For example, banks are constantly under attack mainly due to their digital transformation and use of cloud computing, and according to the research presented at commetric.com (2023), in banks, there is the highest share of phishing, social engineering fraud, ransomware, and the use of trojan horses. However, cyberattacks cause a loss of reputation. Clients may doubt the organization´s ability to protect their sensitive data, which reduces the credibility of the organisation on the client side.

The issue of cybersecurity currently affects everyone who uses the network or devices connected to it. Particularly at risk are those who are in possession of a range of data that are potentially valuable to criminals, i.e., data that may represent trade or business secrets. Data that, once stolen, could be the basis for extortion actions or inducing the payment of a ransom for its recovery or nonpublication. This is therefore the case not only for critical infrastructure entities but also for companies such as law firms and consultancies, including those specialising in public relations. And these are the ones that often have confidential information that customers share with them. Hu proposed a research model based on comparing the benefits of using co-created value in social networks and the risk of leaking sensitive data and loss of privacy. However, they point to the paradox that despite growing concerns about cybersecurity, the number of social media users is on the rise. This paradox illustrates the interactive process of cognitive/behavioural balance between cybersecurity consideration and co-creation of value through the use of social networks (Hu et al., 2018). When examining perceived cybersecurity concerns, they distinguished two dimensions, namely information security in the sense of protecting personal data and privacy, in the sense of the extent of user control over their personal data (Bansal, 2017).

The loss of a substantial amount of personal or sensitive data can have severe consequences for organisations due to its significant impact: damage to organisations can take the form of physical, digital, economic, psychological, social, and societal harm, as well as reputational damage (Agrafiotis, Nurse, Goldsmith, Creese, Upton, 2018). Part of reputational damage is, for example, damaged public perception, loss of key staff, loss of certifications, or damaged relationships with stakeholders. However, each interested subject can perceive damage differently, and therefore risk management, including cyber insurance within the context of cyberspace, is an integral part of an organisation´s processes (McGregor, Reaiche, Boyle, de Zunielqui, 2023).

An important aspect when researching cybersecurity is also awareness of the risk of reputation damage in the event of information leakage, which is especially important when building the brand of PR agencies. Information leaks can be insidious and intentional, but sometimes leaks of an unintentional nature can also occur. Regardless of the type of breach, Knight and Nurse (Knight and Nurse, 2020) provide a framework for effective communication and rebuilding trust after a security incident. This consists of framing the message, deciding when to disclose, how to disclose, and preparing for reaction. It also contains the guidelines for delivering the message. The biggest problem of cyberattacks is the potential for reputational damage. PR agencies must try to prevent cyberattacks, e.g. consider what types of information they will publish as part of PR, i.e. to avoid publishing internal emails, avoid phishing, etc. In the event that an attack occurs, it is important to answer basic questions, but the information should come from one source. Official communication also reflects the cultural dimension, in terms of preferences for

individualism or collectivism, power distance, and also communication style in terms of preference for low-context or high-context communication (Kim, Lee, 2018).

A significant threat in addition to attacks conducted online is lack of knowledge or ignorance, as well as lack of awareness of threats (Hoffmann, 2018). Therefore, the implementation of solutions to secure the organisation should be part of the management processes of modern companies.

Franco et al. (Franco, Lacerda, Stiller, 2022) emphasise the necessity of investments in cybersecurity and offer a six-phase framework for the creation, implementation, and operation of a cybersecurity strategy in small and medium-sized enterprises. Training of employees is an important part of the implementation of the cybersecurity project. PR agencies could also follow these steps to support and manage cybersecurity projects effectively.

Krawczyk-Sokołowska and Caputa (Krawczyk-Sokołowska, Caputa, 2023), using the example of the analysis of the purchasing process in the electrical trade in Poland, point out that it is necessary to consider not only the benefits of social networks for interested parties, but also the threats that online relationships bring. Cybersecurity in this context can be based on the triad: (i) perception, defined as the ability to recognise potential risks from online relationships and assess their likelihood of occurence; (ii) action, defined as the capability to implement protective measures and utilise safeguarding technologies; and (iii) knowledge, defined as the proficiency in using technological means to ensure the security of such relationships. Increasing awareness of the potential of networks and identifying risk factors associated with them is important nowadays. Digital activities should not revolve solely around acquiring IT skills or building relationships (Krawczyk-Sokołowska and Caputa, 2023). Enterprises must establish a culture of network security and also educate employees in this field. The example of banks that educate not only employees but also clients can be an inspiration. Banks constantly draw attention to cyber risks, thus essentially they educate clients.

Sarabi et al. (Sarabi, Naghizadeh, Liu, Y., Liu M., 2016) aimed to determine the extent to which details about an organisation help assess the risk of information leakage. They claim that it is possible to predict incidents with relatively high accuracy, but it is not possible to predict the type of incident unequivocally. However, they focused on the types of incidents by action, actor, and asset type, whilst not taking into account e.g. region or industry.

Security is not only about protecting data, knowledge, and information resources. It is also financial security. The authors of the IBM report indicate that the construction of incident response structures or the regularly conducting tests of the effectiveness of the information security management system has an impact on the fact that the level of losses between an enterprise that has implemented such measures and an enterprise that has not decided to introduce them is, on average, USD 2 million (Piecuch, 2020). With this in mind, it is important to note that the effectiveness of security measures must manifest itself in proactivity. Security must be proactive. This means that systems must be designed and tested with security in mind from the outset (Kemmerer, 2003).

The topic of cybersecurity is also gaining particular importance for another reason, namely the growing discussion of technologies used within the framework of artificial intelligence. The problem of phishing seems to be becoming even more serious, as even solutions such as ChatGPT can be involved in the creation of manipulative, persuasive content, the kind that can ultimately influence the awareness of recipients in order to obtain data from them, which can then be used to steal or extort data necessary for further criminal

activities. Increased vigilance and a reinforced commitment to thorough fact-checking become imperative when using ChatGPT to create content based on web searchers (Gaule, 2023). But on the other hand, also ChatGPT has the capability to generate cybersecurity scripts, so it can be a tool to help strengthen security (Mijwil et al., 2023). In general, artificial intelligence tools (e.g. Crowdstrike) used in cybersecurity are complex to adopt as their implementation require specialist knowledge. The output accuracy is high, although it depends on the threats and sophistication of the systems. AI tools definitely enhance security efforts, but there are still limitations due to evolving threats (Gaule, 2023). Building protection systems is a basic principle to gain clients' trust (Aji et al., 2023). For example, the introduction of chatbots can raise concerns about privacy, security reliability, as well as potentially inaccurate and misleading information.

The issue of cybersecurity is significant in various types of organisations, including municipalities (Vestad, Yang, 2023). Several challenges related to cybersecurity are also faced by the public relations industry today, because they work with the data of other people. This applies both to executive areas, the actions taken by practitioners and academics in this field, and also to the people who work in PR. The first issue mainly refers to problems related to content creation and its appropriate security, while the second, among others, refers to awareness, understanding of the challenges, and the need to secure the value that data and information can and do represent.

2. KNOWLEDGE AND EXPERIENCE IN CYBERSECURITY AMONG PUBLIC RELATIONS PROFESSIONALS IN POLAND

The survey on the perception of cybersecurity by public relations professionals in Poland was carried out by the Polish Press Agency and a team of analysts from the Information Society Development Institute. The project was carried out using a quantitative method, using the CAWI technique in 2022 on a sample of 119 professionals, mainly specialists and experts in the databases of the Information Society Development Institute. The survey questionnaire asked questions about knowledge of types of cyberattacks and on-line activities, experiences of cyberattack, the topic of securing data, participation in data security training, sources of knowledge on cyberattack threats or frequency of cybersecurity activities. The structure of the questions was mainly based on rank-order scales. The analyses performed are based on frequency distributions and the procedure of comparing averages in independent groups. The set of factors on the basis of which statistical diversification procedures were carried out is composed of variables such as gender, age, recommendation of PR work to friends and family, education, completed PR studies or courses, years in the industry, position in the organisation, main workplace, size of the main workplace organisation and experience of a crisis situation by the organisation in the last 12 months.

Surveys conducted among public relations professionals in Poland indicate that they have all heard of hacking, as an unlawful activity by which an unauthorised person gains access to information and data or gains access to information network systems. 98.3% of the respondents know about phishing and pharming, while 87.4% of the respondents know about malware. A similarly large group of respondents (73.1%) have heard of sniffing, while concepts such as ransomware or DoS/DDoS are known to a relatively smallest percentage of respondents – 63.9% and 54.6% of affirmative indications, respectively.

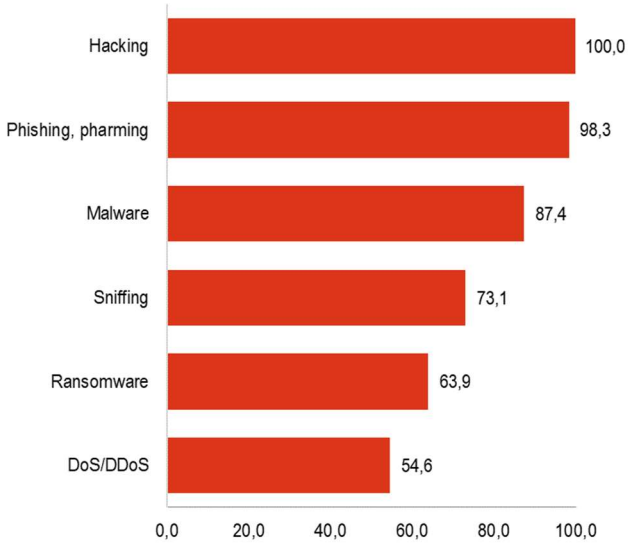

Figure 1. Have you heard of the following types of cyber-attacks online? N=119 (in % of affirmative answers)

Source: own research.

When making intergroup comparisons, it can be observed that persons with seniority of more than 3 years were significantly more likely to declare knowledge of the terms phising, pharming – 100% compared to 93.3% among persons with seniority of up to 3 years. Knowledge of the term malware was significantly more frequently indicated by persons up to 35 years (94.8% vs. 80.3% among older persons), while knowledge of (distributed) denial-of-service attack was indicated by men (69.8% vs. 46.1% among women). Male respondents (88.4% vs 50% of females), those 35+ years of age (73.8% vs 53.4% of younger respondents), those with more than 10 years of industry experience (78.3% vs 36.7% of those with up to 3 years of experience) and those in management positions (88% vs 45.7% of those in executive positions) were significantly more likely to be familiar with the concept of ransomware.

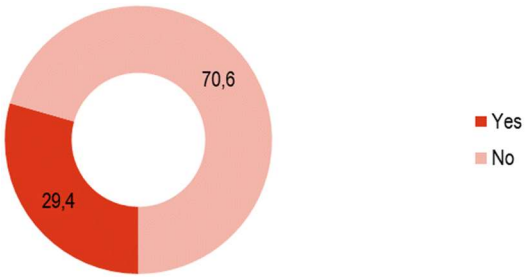

Figure 2. In the last month, have you encountered an attack aimed at deleting or intercepting data that directly affected you? N = 119 (%). The values in the graph have been rounded, so they may not be 100%

Source: own research.

Almost one in three respondents had experienced a direct attack aimed at deleting or intercepting their data in the month preceding the survey, 29.4%. Comparing the experience of a direct attack mentioned above with the profile of the respondents, we observe that it was significantly more often experienced by the male respondents (44.2% against 21.1% female) and those working in companies with 250 or more employees (52.4% against 10.5% in companies with up to 9 employees).

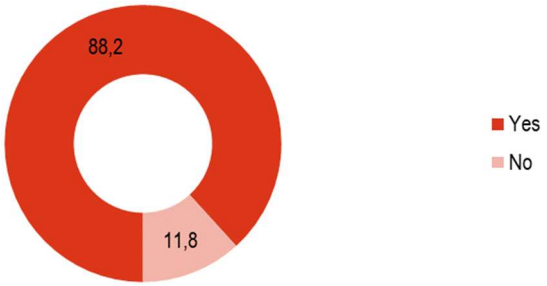

Figure 3. Do you protect/secure your data on the Internet/stored on your private/service computer? N=119 (in %). The values in the graph have been rounded, so they may not be 100%

Source: own research.

Almost nine out of ten public relations professionals surveyed declared that they protect their data. This applies to their own data located on the Internet (e.g. access data) as well as that located on a private/service computer, 88.2%. 11.8% of the respondents do not use security. The issue of data protection/security was not differentiated by any of the variables characterising the profile of the public relations professionals surveyed.

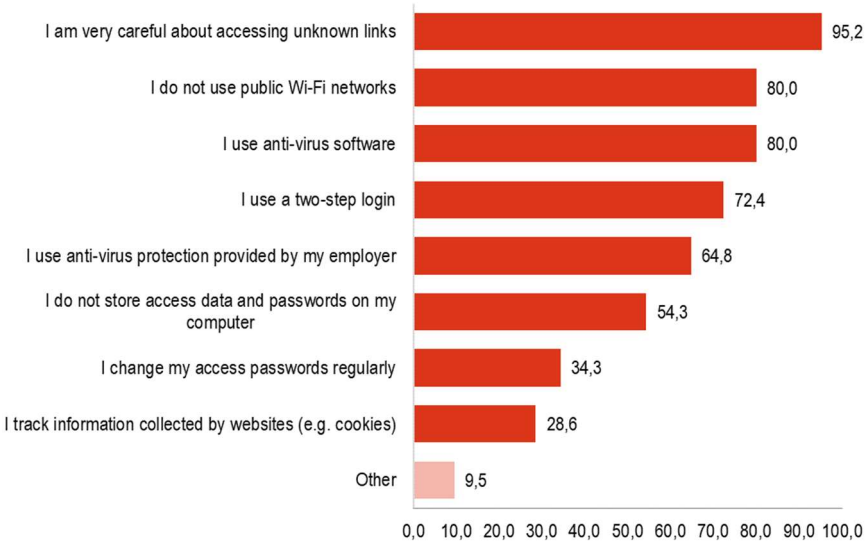

Figure 4. How do you protect/secure your data? N=105 (in %, multiple choice)

Source: own research.

In terms of data security methods used by respondents, almost all PRs declared that they are cautious when accessing unknown links, 95.2%. Four out of five respondents also admitted that they do not use public Wi-Fi networks and use anti-virus software. It was relatively less common for respondents to indicate that they monitor the information collected by websites, 28.6% of affirmative indications. Those with tertiary education were significantly more likely to declare that they are cautious when accessing unknown links – 97.7% compared to 75% among those with secondary education. The monitoring of the information collected on the websites was significantly more often declared by respondents aged 35+ (38.2% vs 18% among younger respondents), with more than 10 years of experience (38.1% vs 7.1% among those with up to 3 years of experience) and in management positions (41.7% vs 14.6% among those in executive positions). Significantly more likely to change their passwords regularly were those over 35 years of age (43.6% vs 24% among younger people), those with a degree in PR, courses, etc. (42.6% vs 21.4% among those without), with 4-10 years of experience (42.9% vs 14.3% among those with up to 3 years of experience), working in a place other than PR agencies (51.1% vs 21.7% in PR agencies) and in companies with 250 or more employees (66.7% vs 16.4% in companies with 10-49 employees).

Figure 5. What data do you protect/secure? N = 105% (%, multiple choice)

Source: own research.

When analysing the declarations regarding the data that the surveyed public relations professionals protect/secure online, it can be seen that the highest percentage of indications concerned access data to bank accounts, 92.4%. More than four in five respondents secure access data to social networks (81.9%), to the company's editing and CMS systems (81%) and personal data (81%). The relatively smallest percentage of indications concerned the protection of access data to external resources, 41%. Securing access data to online stores was declared significantly more often by men (65% vs 44.6% among women), and by those

who would not recommend working in PR to their family/friends (72% vs 41.1% among those recommending this profession), with more than 10 years of experience in the industry (69% vs 32.1% among those with up to 3 years of experience), in executive/management positions (65% vs 36.6% in executive positions) and working elsewhere than in a PR agency (64.4% vs 43.3% in PR agencies).

Further analysis showed that access data to external resources is significantly more likely to be protected by men (55% vs 32.3% among women), those aged 35+ (50.9% vs 30% among younger people), those with more than 10 years of industry experience (57.1% vs 17.9% among those with up to 3 years of experience) and those in executive/management positions (55% vs 22% in executive positions).

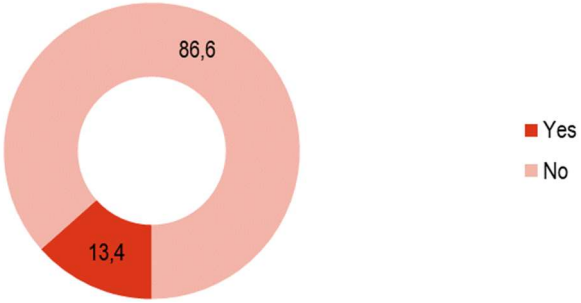

Figure 6. Have you ever lost important data? N=119 (in %). The values in the graph have been rounded, so they may not be 100%

Source: own research.

The vast majority of public relations professionals declared that by the time of the survey they had never experienced the loss of important data, 86.6%. 13.4% of the respondents had such experiences. None of the independent variables describing the profile of PR professionals surveyed statistically significantly differentiated issues related to the loss of important data.

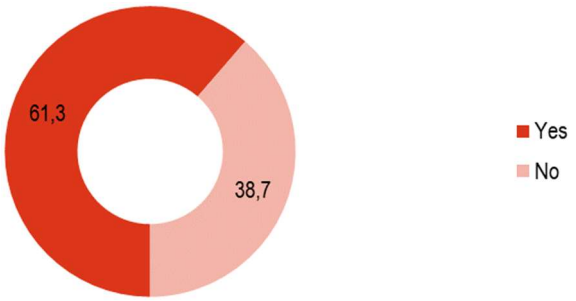

Figure 7. Does your company keep employees informed about threats and instructs them how to protect themselves? N=119 (in %). The values in the graph have been rounded, so they may not be 100%

Source: own research.

Three out of five respondents said that their company keeps employees informed about risks and instructs them on how to protect themselves, 61.3%. We note that those over the age of 35 (77% vs 44.8% among younger respondents), not recommending working in PR to their family/friends (73.7% vs 42.1% among those ambivalent), working in companies with 250 or more employees (85.7% vs 47, 4% in companies with up to 9 employees) and those who had not experienced an image crisis in the year preceding the survey (68.8% vs 23.1% in companies with no knowledge of the subject) were significantly more likely to declare that the entity they work for keeps them informed of threats and instructs them on how to protect themselves.

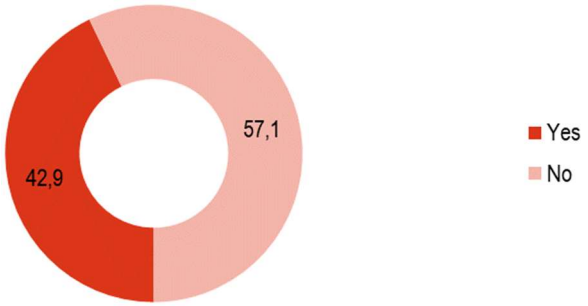

Figure 8. Have you attended any data security training? N=119 (in %). The values in the graph have been rounded, so they may not be 100%

Source: own research.

More than two in five respondents declared that they had attended a data security training course – 42.9%. This was significantly more often declared by respondents over 35 years of age (59% vs 25.9% among younger respondents), those employed elsewhere than in PR agencies (53.8% vs 34.3% in PR agencies) and employees of companies with 250 or more employees (71.4% vs 26.3% in companies with up to 9 employees).

When analysing and identifying the sources of knowledge from which respondents obtain their knowledge on cyber threats, it can be observed that the highest percentage of indications concerned the Internet – 89.1%. Almost half of the respondents seek knowledge in this area through social media – 47.9. They rarely obtain knowledge about cybersecurity from television and radio – 6.7% and 0.8% of indications, respectively.

It should be noted that women are significantly more likely to learn about cyber threats from family members (14.5% vs. 2.3% among men). Acquaintances were significantly more often indicated by women (28.9% vs 11.6% among men), people up to 35 years of age (34.5% vs 11.5% among older people), with up to three years of work experience in the industry (43.3% vs 10.9% among those with more than 10 years of experience) and in executive positions (34.8% vs 12.5% in management positions). Those employed in PR agencies are significantly more likely to derive knowledge in this aspect from their colleagues – 28.4% vs. 11.5% of those employed in other jobs. Those with seniority in the PR industry of more than 10 years (19.6% vs. 0% among those with seniority of up to 3 years) and those not working in PR agencies (17.3% vs. 6% in PR agencies) are significantly more likely to use the press in this regard. General knowledge was significantly more often indicated by those without PR degrees, courses, etc. (41.3% vs 22.5% among those with them). Respondents over 35 years of age (29.5% vs 10.3% among

younger respondents), those with a PR degree (26.8% vs 10.9% among those without one), those employed in places other than a PR agency (34.6% vs 9% in PR agencies) and in companies with at least 250 employees (47.6% vs 8.2% in companies with 10–49 employees) are significantly more likely to derive their knowledge from training.

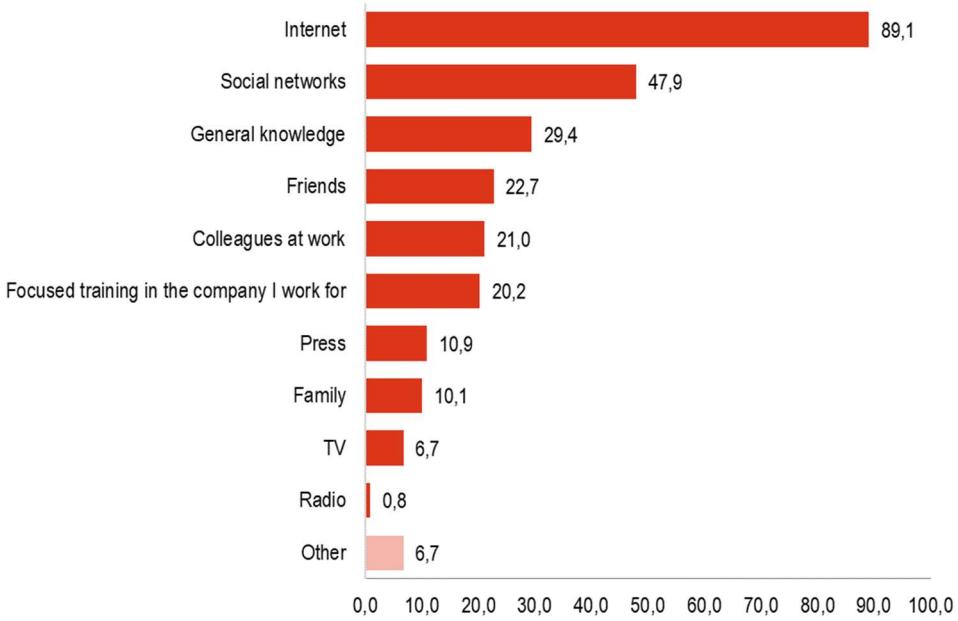

Figure 9. From what sources do you most often draw your knowledge of cyberattack threats? N=119 (%, multiple choice)

Source: own research.

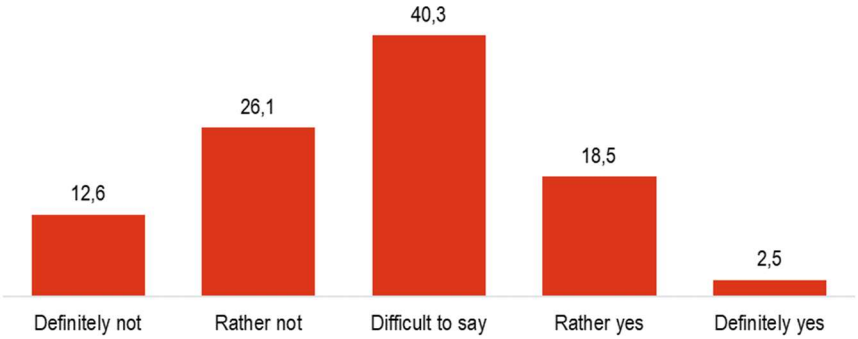

Figure 10. In your opinion, are the companies in your industry in Poland well protected against cyber attacks? N=119 (in %). The values in the graph have been rounded, so they may not be 100%.

Source: own research.

More than a fifth of the respondents were of the opinion that PR firms in Poland are well protected against online attacks – 21%. 38.7% of the respondents expressed the opposite opinion, while 40.3% of the respondents were unable to clearly state their opinion on this issue. None of the independent variables statistically significantly differentiated the question of whether PR firms in Poland are well protected against cyber attacks.

Referring to individual situations related to cybersecurity, respondents declared that they have observed an increase in online threats related to data loss or takeover in recent years, with a mean of 4.44 on a scale of 1–5 (Figure 11). Respondents were just as often of the opinion that they knew how to recognise threatening emails – mean 4.21. Against this backdrop, respondents were far less likely to say that they use the same login password everywhere and to agree that cybersecurity is more of a fashionable topic than a real necessity – means of 1.82 and 1.61 respectively.

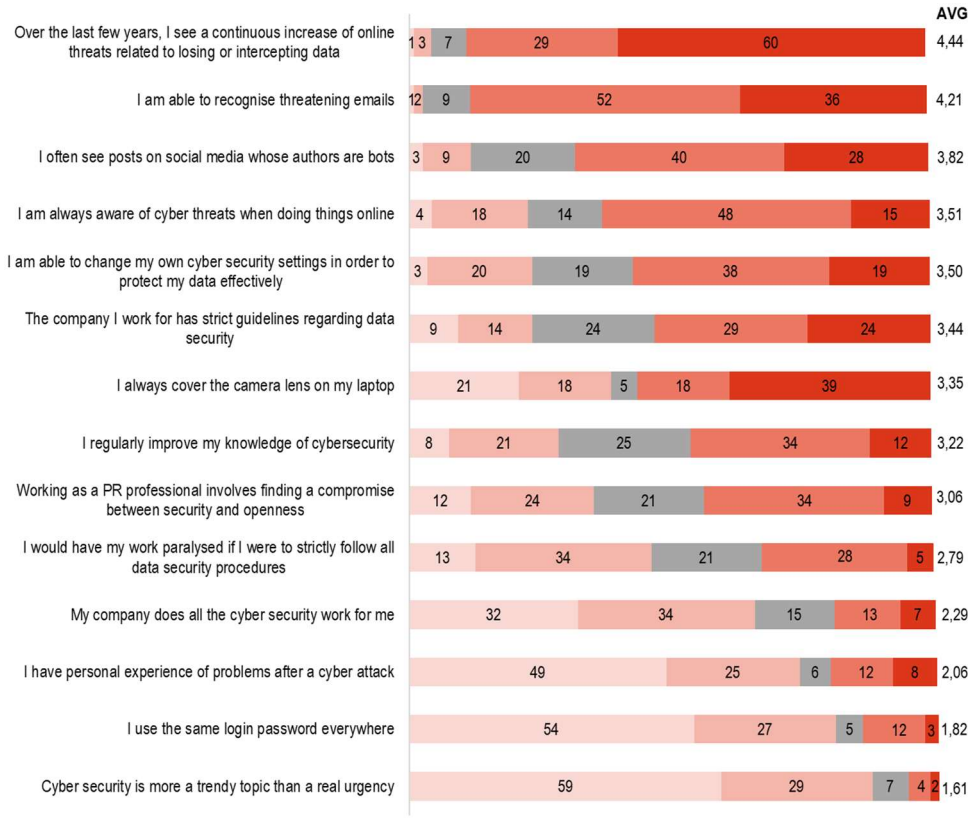

Figure 11. Comment on the following situations, N=119 (in %). The values in the graph have been rounded, so they may not be 100%

Source: own research.

When making cross-group comparisons, it can be observed that those 35 and under were significantly more likely to say that if they were to strictly apply all data security procedures, their work would be paralysed, 3.05 vs 2.54 among older people). The ability

to recognise emails at risk was significantly more often indicated by respondents with 4-10 years' seniority in the industry, 4.42 versus 3.93 among those with up to 3 years' seniority. Men (3.84 vs 3.30 among women) and those who did not recommend PR work to family/friends (4.00 vs 3.05 among those ambivalent) were significantly more likely to declare that they were able to change their own Internet security settings to effectively protect their data.

Those recommending PR work to family/acquaintances were significantly more likely to believe that they have seen a steady increase in online threats related to data loss or interception over recent years - 4.65 against 4.13 among those who were ambivalent. Respondents over the age of 35 years (3.79 vs. 3.07 among younger respondents) and those working in companies with 250 or more employees (4.14 vs. 3.00 in companies with 0-9 employees) were relatively more likely to admit that their companies have strict guidelines regarding data security. PR professionals with more than 10 years' seniority in the industry were significantly more likely to say that they often see posts on social media that are authored by bots, 4.09 compared to 3.47 among those with up to three years' seniority.

Those who recommended PR jobs to family/friends were significantly more likely to say that they always cover the camera lens on their laptop, 3.81 vs 2.74 among those who did not recommend PR jobs. Having personal experience of problems after a cyber attack was relatively more often indicated by respondents aged 35+ (2.30 vs 1.81 among younger respondents) and those with a degree in PR, courses, etc. (2.30 vs. 1.72 among those without them). Men (3.51 vs 3.05 among women), those over 35 years of age (3.51 vs 2.91 among younger people) and those with at least a doctorate (4.27 vs 2.78 among those with secondary education) were significantly more likely to declare that they regularly expand their knowledge of cybersecurity.

Respondents with up to three years of work experience in the industry admitted the use of the same login password significantly more frequently – 2.20 vs. 1.48 among those with more than 10 years of experience. On the contrary, women (2.54 vs 1.84 among men), those with secondary education (2.67 vs 1.36 among those with at least a PhD) and those in executive positions (2.59 vs 1.60 among those in management positions) were significantly more likely to admit that their company does all the cybersecurity work for them.

3. SUMMARY

Cybersecurity is one of the critical elements for maintaining the continuity of a company's operations, its ability to generate revenue, and often maintaining its level of competitiveness in the market, e.g. financial (Piecuch, 2020).

Surveys conducted among public relations professionals in Poland indicate that this is a topic they already recognise and are largely involved in securing data and information. The respondents are aware. They indicate that they have heard of hacking, to a lesser extent of phishing, pharming, malware, and sniffing. They are less aware of topics such as ransomware or DoS/DDoS. The vast majority of the public relations professionals surveyed declared that they secure data on the Internet and on their private/service computer, and in terms of the methods used to secure data, almost all declared that they are cautious and do not access unknown links. The same is true for the data that respondents secure online, such as bank accounts, social media access data, the company's editing and CMS systems, or personal data.

An important part of the overall process of building awareness and skills related to cybersecurity is training and information. Most of the respondents indicated that their employers inform them about the risks and instruct them on how to protect themselves. In addition to this, the respondents do their own further training. They obtain their knowledge about risks on the Internet, including social networks, and general knowledge.

In view of a number of findings from the survey of public relations professionals, it can be concluded that awareness of threats and cybersecurity is high. It can also be assumed that the respondents representing this environment have knowledge and, above all, understand the need for various types of security measures for themselves, as well as their employers and the clients they work with. However, this topic requires further exploration because of the dynamically changing reality in this area.

REFERENCES

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D. (2018). *A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate*. *"Journal of Cybersecurity"*, Vol. 4(1). DOI: 10.1093/cybsec/tyy006.

Ahmad, R., Alsmadi, I., Alhamdani, W., Tawalbeh, L. (2023). *Zero-day attack detection: a systematic literature review*. *"Artificial Intelligence review",* Vol. 56.

Aji, G.G., Widod S., Aji, G.N., Aji, G.G., Prawitasari, D. (2023) *Building trust in the digital age: How HRM and cybersecurity collaborate for effective stakeholder relations. "Management Analysis Journal"*, Vol. 12(2).

Bansal, G. (2017). *Distinguishing between privacy and security concerns: an empirical examination and scale validation. "Journal of Computer Information Systems"*, Vol. 57(4).

Commetric. (2023). *Is Banking´s Crisis PR Stuck in the Stone Age? Why Media Analytics is Crucial for Today´s Cybersecurity Challenges.* Access on the internet: https://commetric.com/2023/09/18/is-bankings-crisis-pr-stuck-in-the-stone-age-why-media-analytics-is-crucial-for-todays-cybersecurity-challenges/.

Chałubińska-Jentkiewicz, K. (2019). *Cyberbezpieczeństwo – zagadnienia definicyjne*. *"Cybersecurity and Law"*, Vol. 2(2).

Craigen, D., Diakun-Thibault, N., Purse, R. (2014). *Defining Cybersecurity*. *"Technology Innovation Management Review"*, Vol. 4(10).

Franco, M.F., Lacerda, F.M., Stiller, B. (2022). *A Framework for the planning and management of cybersecurity projects in small and medium-sized enterprises*. *"Revista de Gestão e Projetos"*, Vol. 13(3).

Gaule, H. (2023). *Artificial Intelligence in Public Relations and Communication: An Approach for Integrating AI Education into Communications Curricula* [In:] Adi, A., ed., *Artificial Intelligence in Public Relations and Communications: cases, reflections and predictions*. Berlin: Quadriga University of Applied Sciences.

Hoffmann, T. (2018). *Główni aktorzy cyberprzestrzeni i ich działalność* [in:] Dębowski T., ed., *Cyberbezpieczeństwo wyzwaniem XXI wieku*. Łódź–Wrocław: ArchaeGraph.

Hu, T., Wang, K.-Y., Chih, W., Yang, X.-H. (2018). *Trade off Cybersecurity Concerns for Co-Created Value*. *"Journal of Computer Information Systems"*, Vol. 60(5).

Janczewski, R. (2022). *Cyberbezpieczeństwo w życiu społecznym* [In:] Stala, J., Butrymowicz, M., ed., *W służbie społeczeństwu. Polska w obronie praw człowieka na świecie i w kraju.* Kraków: Wydawnictwo Naukowe UPJPII.

Kaczmarczyk, B., Dobrowolski, P., Dąbrowska, M. (2018). *Wybrane aspekty edukacji dla bezpieczeństwa*. Toruń: Wydawnictwo Adam Marszałek.

Kemmerer, R.A. (2003). *Cybersecurity.* Portland: 25th International Conference on Software Engineering.

Kim, N., Lee, S. (2018). *Cybersecurity Breach and Crisis Response: An Analysis of Organizations' Official Statements in the United States and South Korea*. *"International Journal of Business Communication",* 58(4).

Knight, R., Nurse, J.R.C. (2020). *A framework for effective corporate communication after cyber security incidents*. *"Computers & Security",* Vol. 99.

Korzeniowska, H. (2004). *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*. Kraków: European Association for Security.

Krawczyk-Sokołowska, I., Caputa, W. (2023). *Awareness of network security and customer value – The company and customer perspective. "Technological Forecasting & Social Change",* Vol. 190.

Li, Y. (2011). *Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework*. *"Communications of the Association for Information Systems",* 28(1).

McGregor, R., Reaiche, C., Boyle, S., de Zunielqui, G.C. (2023). *Cyberspace and Personal Cyber Insurance: A Systematc Review*. *"Journal of Computer Information Systems".* DOI: 10.1080/08874417.2023.2185551.

Mijwil, M.M., Aljanabi, M., Hussein, A. Ali (2023). *ChatGPT: Exploring the Role of Cybersecurity in the Protection of MedicalInformation*. *"Mesopotamian Journal of CyberSecurity".* DOI: 10.58496/MJCS/2023/004.

Nguyen, D. (2023). *How news media frame data risks in their coverage of big data and AI*. *"Internet Policy Review",* Vol 12(2). DOI: 10.14763/2023.2.1708.

Piecuch, I. (2020). *Cyberbezpieczeństwo w czasach kryzysu*. *„Nowa Energia"*, Vol. 4(74).

Radhi, M.A.H., Hussien, N.M., Mohialden, Y.M. (2023). *Reviewing Organized Crime: A Global Perspective on Cyber Security*. *"Scientific Research Journal of Engineering and Computer Science",* Vol. 3(4).

Sarabi, A., Naghizadeh, P., Liu, Y., Liu, M. (2016). *Risky business: Fine-grained data breach prediction using business profiles*. *"Journal of Cybersecurity",* Vol. 2(1).

Veale, M., Brown, I. (2020). *Cybersecurity. "Internet Policy Review"*, Vol. 9(4).

Vestad, A., Yang, B. (2023). *Municipal Cybersecurity – A Neglected Research Area? A Survey of Current Research* [In:] Onwubiko, C. et al., ed., *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*. Singapore: Springer Proceedings in Complexity.