THE HUMAN FACTOR IN THE SECURITY OF INFORMATION RESOURCES OF MARKETING DEPARTMENTS AT UNIVERSITIES IN POLAND, UKRAINE AND THE CZECH REPUBLIC

DOI: 10.33141/po.2023.04.37

Organization Review, No. 4(999), 2023, pp. 359-367

www.przegladorganizacji.pl

Paweł Kobis
Artur Kisiołek
Oleh Karyy
Adam Pawliczek

Introduction

The security of information resources is currently one of the main factors that ensure that an organisation can operate properly. This is due to the fact that the potential of a modern organisation, which guarantees its competitiveness, is accumulated in its information resources, including patents, service databases and proprietary marketing methods etc. (Brzeziński, 2023). Every kind of organisation, including a university, also processes information related to personal data, which, depending on the country, is subject to specific legal protection. Any information security incident may result in the seizure of intangible assets by third parties (e.g., competitors), their destruction or disclosure to the public. Consequently, an economic entity is exposed to situations like:

- Loss of key information that distinguishes it from other organisations in the economic market;
- Loss of credibility and reputation (e.g. publication of a list of their logins and passwords);
- Legal and financial sanctions (leakage of protected personal data).

Nowadays, information resources are, to a large extent, stored in the IT system, which may consist of several sub-systems working within the LAN, such as: ERP (Enterprise Resources Planning), CRM (Customer Relationship Management), LRP (Logistic Resource Planning) and many others. In the optimum working environment, these sub-systems exchange information with each other using integrated databases at the same time.

The main „foundation" of information security systems are software and hardware solutions. They automatically prevent illegal interference from the external network (Internet) and possible sabotage activities from the internal network (LAN). Hardware and software protection is currently additionally supported by a number of processes, e.g. cyclical risk analysis, usually based on the ISO 27005 standard, training in the field of information security and simulation of cyber-attacks.

All the above methods of protection are very effective in eliminating threats originating from the Internet, caused by viruses, malware, ransomware etc., which may be introduced into local networks using phishing techniques or imitating known applications, etc. Regular training and attack simulations provide additional knowledge for people working to process information resources securely.

The level of security within organisations and universities that take cybersecurity seriously is currently quite high. It is difficult for unauthorised persons to breach security in order to obtain specific information resources. This is why the human factor is an increasingly popular way to „bypass" security. This method is based on exploiting human weaknesses, habits, character traits and lack of competence to circumvent the technical security of systems (Kobis, Kisiołek, 2018, p. 45). The human factor often randomly generates dangerous situations not caused by external interference, exposing intangible resources to destruction or making them available to third parties.

The aim of the article is to present the human factors that most often cause threats to intangible resources. The authors have presented the perception of individual human factors by people from marketing departments regarding their threat to intangible resources, and answers from respondents from Poland, Ukraine and the Czech Republic have been presented and compared.

Human factors causing a risk to intangible resources

When analysing the literature on human factors affecting the security of intangible assets, eight main factors can be identified (Alavi i in., 2013; Ani i in., 2019; Ghafir i in., 2018; Kobis, 2021; Kobis, Karyy, 2021; Sedgwick, 2019):

1. Uniformity of duties
2. Rush and fatigue
3. Excessive trust in relation to third parties
4. Excessive talkativeness generally accepted
5. Susceptibility to social engineering activities
6. Dissatisfaction with generally accepted working conditions
7. Deliberate actions supported by a rival university (economic espionage)
8. Lack of sufficient knowledge of information protection rules

The monotony of performed duties is also referred to in the literature as monotony of work. It is considered to be one of the most common causes leading to mistakes in various areas of duties, not only those related to information management. The monotony of work is a universal phenomenon in terms of the types of areas in which mistakes are made (Kobis, 2021, p. 300). The same factor can be the cause of a risk in information security, as well as risks included in health and safety regulations. The monotony of work is also mentioned in the Labour Code, e.g. the fourth section entitled „Obligations of the employer and the employee", Chapter 1 of Article 94 Point 2a reads: „*In particular, the employer is obliged to: (...) organise work in such a way as to reduce the burden of work, especially monotonous work as well as work at a predetermined pace*" (Sejm Rzeczypospolitej Polskiej, 2019, p. 31). This means that an employer who deliberately exposes an employee to monotonous work is also held responsible for the potential consequences of this decision.

Attempts to mitigate the negative effects of the factor described above may include (Kołodziejczyk, 2017; Konarska, 2003, p. 16):

- Conducting training on how to counteract monotony and its effects;
- Changes to how work is organisation;
- Labour turnover;
- Implementing additional tasks to be performed by employees and changing the rhythm of activities (not necessarily required in the working process);
- Introducing additional breaks at work that require a different activity from what is routinely done during professional work.

The way in which the factor „Rush and fatigue" arises and develops may have different origins and is more an area of research in other scientific disciplines: sociology, medicine, psychology. However, when applying it to the aspects of ensuring secure information management, it is impossible not to distinguish several possible scenarios of its escalation. In addition to temporary indispositions of the employee, which may affect the way he or she processes information, the most common scenarios that appear in the security literature are (Kobis, 2021, p. 287):

- Information fatigue syndrome;
- Excessive workload;
- Excessive hourly workload at work.

As M. Czernecka et al. (2017, p. 2), a psychologist and efficiency expert, writes in a report entitled „Work, power, energy in Polish companies. Six Areas That Affect the Effectiveness of an Organisation": „Modern work rules tell us to do more and faster. Every day, we receive a huge amount of data that we need to efficiently and flawlessly „handle": analysing, making appropriate decisions, passing them on or implementing them. We have more and more things to do and a growing sense that we have to work longer hours not to be „left behind". This creates tension, frustration, impatience, irritation, and even fear. We don't even realise that this way of doing things blocks us (and our colleagues) from having a clear, logical, and reflective mindset, which is essential for us to achieve a high level of efficiency. (...) More than half of employees start their day with optimism and enthusiasm, but more than 40% often feel irritated, frustrated and impatient during the day, and a third (32.3%) are tired and discouraged at work". This quote essentially describes the essence of the discussed factor, which may affect the increase in the number of errors made at work, including those directly related to a breach of information security.

Trust in third parties is another factor that puts intangible assets at risk. This factor often results in information being made available to third parties even though they should not have received it or should, at least, have formally requested. The desire to help and trust is often used by people contacting a potential victim via phone, email or chat. A person who trusts an interlocutor, who usually claims to be a customer, business partner or a person of social trust, transfers intangible assets or credentials to them, thus risking their potential destruction or loss.

Another factor, „Excessive talkativeness" has a colloquial dimension, as does „chatter" or „verbosity". It describes a person who finds it difficult to control the excess of words spoken; this is what is called: „saying one word too many". In this way, you can betray a certain secret or abuse someone's trust (Pufal, 2014). The Great Dictionary of the Polish Language (2014) defines „talkativeness" as „the tendency to talk too much and unnecessarily". This feature, which some employees do have, is highly undesirable from the point of view of information security. It is particularly dangerous when combined with social engineering techniques.

Employees with this character trait can be manipulated and „forced" to disclose certain trade secrets in a relatively short period of time by people experienced in social engineering activities. In addition, these people tend to bring up professional matters in private relationships, which further increases the risk of disclosure of certain information. From the point of view of the security of intangible resources and the preservation of secrets in relation to protected subjects, A. Żebrowski (2016, p. 22) considers excessive talkativeness to be even a symptom of recklessness. Thus, such persons should not be given the opportunity to apply for a position requiring the employee to maintain a certain level of confidentiality in the scope of their duties at recruitment level.

Another factor is susceptibility to social engineering activities. In the field of information security management, social engineering methods usually take the following forms (Ciekanowski i in., 2017, p. 54–55; Mitnick, Simon, 2003, p. 360–361):

- Attempting to impersonate an employee of the company or a person sent by such an employee;
- Attempting to help the employee under certain conditions, arranging a credible situation in advance;
- Attempting to ask for help, e.g. by pretending to be an employee of another department or branch (this is most common in large companies where none of the employees know each other);
- Attempting to pretend to be an expert in a particular field by using specialised phrases and terminology in order to instil confidence in a potential employee (victim of fraud);
- Attempting to pretend to be a person with a high social status or power, in a situation where he or she is not personally known to the victim of social engineering activities;
- Pretending to be a new employee or intern.

In addition to activities in the form of direct contact with employees of enterprises, social engineering activities also take the form of manipulation attempts using various electronic communication techniques. The most commonly used tool for this purpose is e-mail. In addition to activities in the form of direct contact with employees of enterprises, social engineering activities also take the form of manipulation attempts using various electronic communication techniques. The most commonly used tool for this purpose is e-mail. In addition to e-mail, there are also forged text messages, information disseminated through social networks, electronic messengers, etc.

Another factor is „Dissatisfaction with generally accepted working conditions". There are a number of possible reasons for working conditions. The most important and most common are: low pay, dissatisfaction with working conditions, boredom and conflict with the employer or co-workers. These reasons may result in a number of actions on the part of the employee: stealing information, destroying information, sabotage or disregarding the principles of safe processing of intangible assets.

Another factor examined is „Economic espionage", i.e. deliberate actions most often supported by competitors. In a way, it is related to the previous factor of dissatisfaction with generally accepted working conditions. In the relevant literature on the subject, two different forms of this are identified:

- The company employs a person (usually under a contract of mandate) whose purpose from the very beginning is to obtain and transfer classified information to third parties;
- A person is recruited in the company to provide specific information to the competition for appropriate remuneration.

In each of the two cases mentioned above, the organisation, including the university, may be deprived of information resources that are crucial for e.g. marketing activities or allowing for the ongoing implementation of the university's operating processes.

Lack of knowledge is also counted as a human factor. Due to a lack of knowledge, employees may perform actions that damage information resources or not take action to protect intangible assets (Noga, Brzeziński, 2021, p. 30). Lack of knowledge can generate specific actions and behavioural patterns of a human being in the face of information management. In order to eliminate this factor, it is necessary to carry out regular training.

The human factor in information security research at Universities in Poland, Ukraine and the Czech Republic

Research methodology

The survey was carried out from November 2021 to June 2023 as part of research work related to an international, interdisciplinary scientific project entitled „Digital Transformation of University Marketing", with

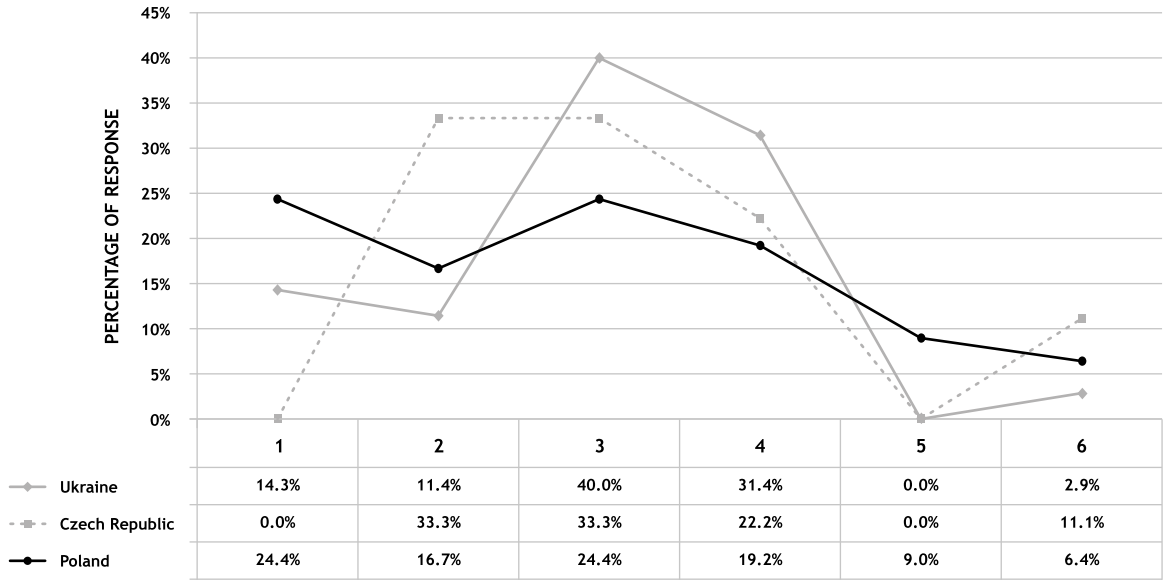
Table 1. Number of HEIs participating in the survey (divided into public and non-public HEIs)

Czech Republic		Poland		Ukraine		Grand Total
Non-public HEIs	Public HEIs	Non-public HEIs	Public HEIs	Non-public HEIs	Public HEIs	
2	7	21	57	4	31	122

Source: own elaboration

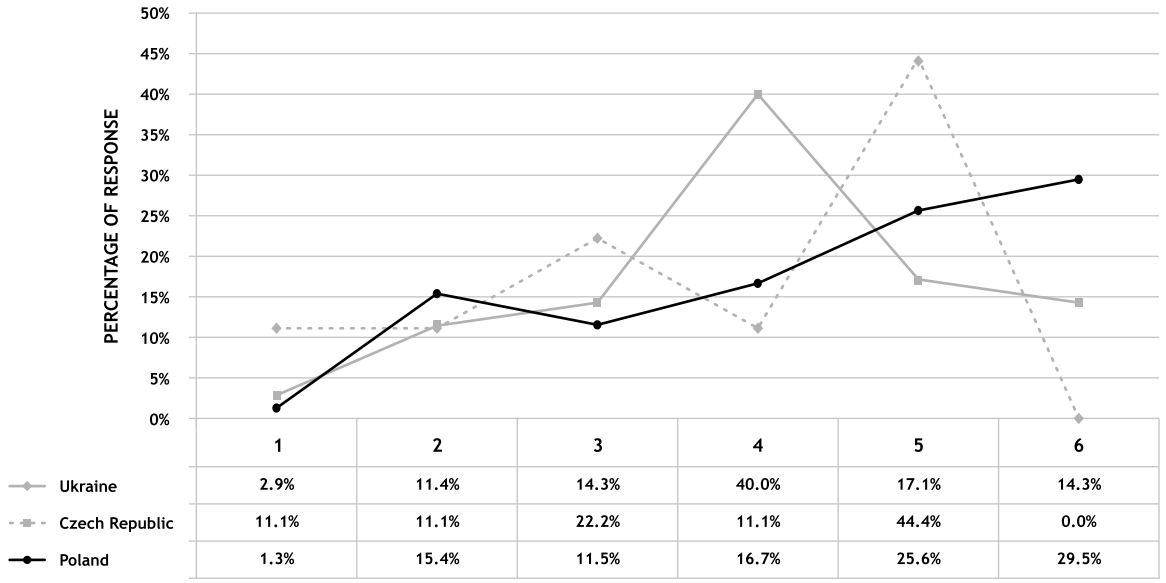
the co-operation of employees of the Faculty of Management at the Czestochowa University of Technology, the Faculty of Economics at the Greater Poland University of Social and Economics in Środa Wielkopolska, the Department of Management of Organisations at Lviv Polytechnic National University in Ukraine and the Department of Business Economics and Management at Moravian Business College in the Czech Republic. The research covered marketing departments of public and private universities in Poland, Ukraine and the Czech Republic. The relatively long period of research was caused by the situation in Ukraine. A total of 122 universities took part in the study, including 78 in Poland, 35 in Ukraine and 9 in the Czech Republic (Table 1). Due to the different representative numbers depending on the country, the results of the surveys are presented as a percentage. The percentages are shown as decimal numbers rounded to one decimal place, in accordance with the recommendations of the American Psychological Association (7th ed.) (APA PsycNET, 2020, p. 179) for group measures.

The research applied in the project included a total of 18 questions from various areas of digital marketing at universities. For the purposes of this article, a question concerning the human factor in information security has been highlighted.



	1	2	3	4	5	6
Ukraine	14.3%	11.4%	40.0%	31.4%	0.0%	2.9%
Czech Republic	0.0%	33.3%	33.3%	22.2%	0.0%	11.1%
Poland	24.4%	16.7%	24.4%	19.2%	9.0%	6.4%

Figure 1. Results for the „Uniformity of performed duties" factor
Source: own elaboration



	1	2	3	4	5	6
Ukraine	2.9%	11.4%	14.3%	40.0%	17.1%	14.3%
Czech Republic	11.1%	11.1%	22.2%	11.1%	44.4%	0.0%
Poland	1.3%	15.4%	11.5%	16.7%	25.6%	29.5%

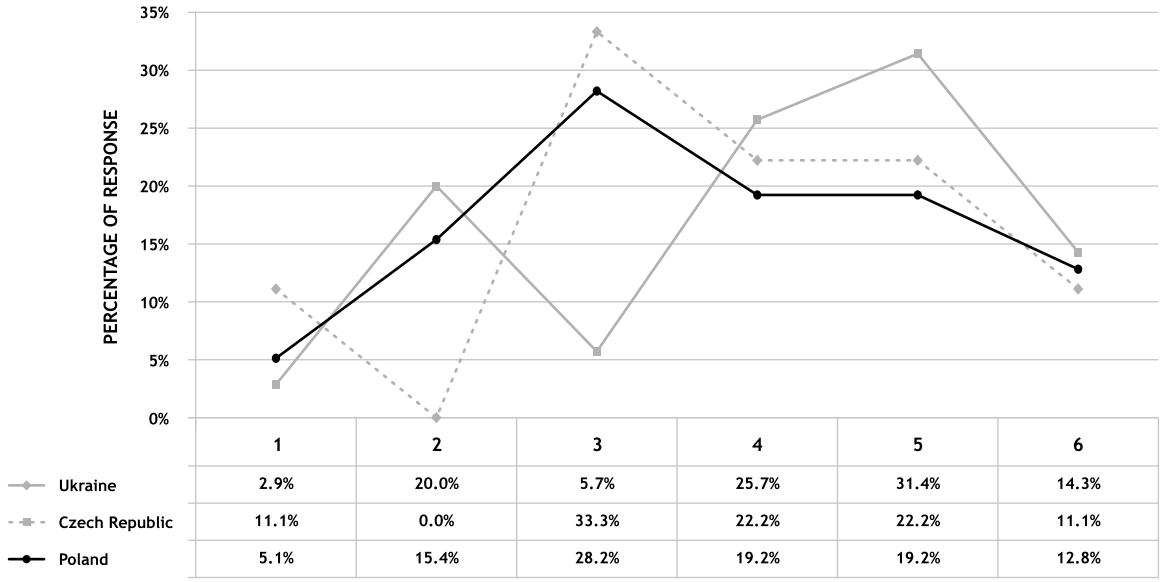
Figure 2. Results for the „Rush and Fatigue" factor
Source: own elaboration

The data was obtained using the CAWI (Computer-Assisted Web Interview) method. The questionnaire form was published on a website specially created for the project. The respondents were people directly involved in managing information resources in the marketing department of a university.

Survey results

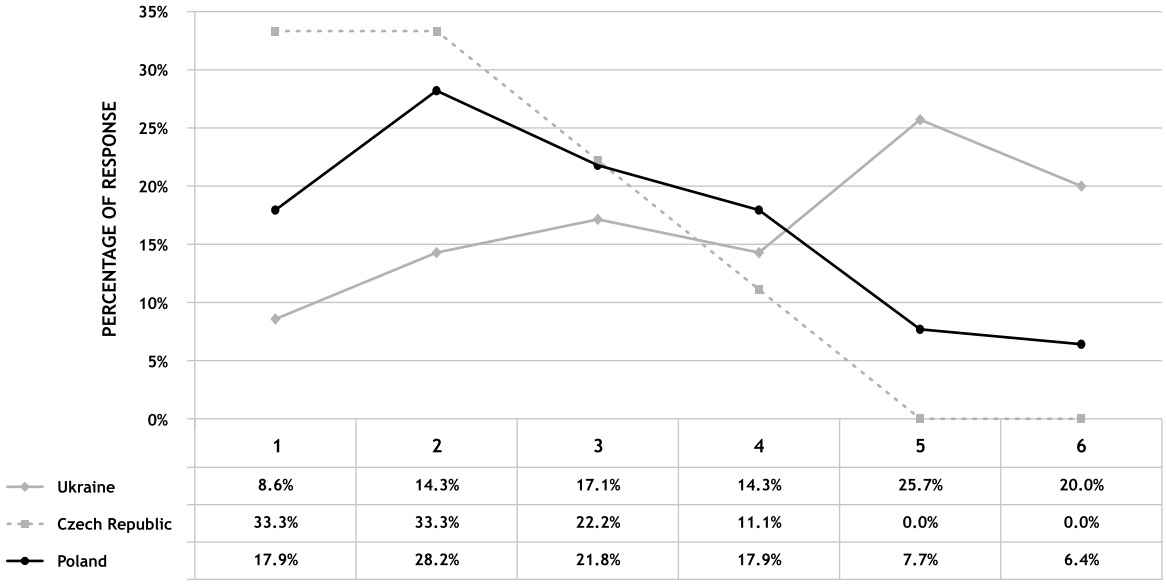
All the presented research results concern the answer to the question: „In your opinion, which of the following human factors and to what extent (on the Likert scale from 1 to 6) can have an impact on the potential damage, deletion or disclosure of data and information to (unauthorised) third parties during e-marketing activities?" Individual responses to the following factors, broken down by country, are shown in Figures 1 to 8.

The first of the factors to be analysed, „Uniformity of performed duties" (Figure 1), was considered by the respondents to have a „medium" impact on the security of information resources in e-marketing processes. The highest score given in each of the countries surveyed was 3, with the highest percentage of respondents giving this score in Ukraine. In Poland, the same factor was given an average score of 1; in the Czech Republic, it was given an average score of 2, which meant that one



	1	2	3	4	5	6
Ukraine	2.9%	20.0%	5.7%	25.7%	31.4%	14.3%
Czech Republic	11.1%	0.0%	33.3%	22.2%	22.2%	11.1%
Poland	5.1%	15.4%	28.2%	19.2%	19.2%	12.8%

Figure 3. Results for the „Excessive trust in third parties" factor
Source: own elaboration



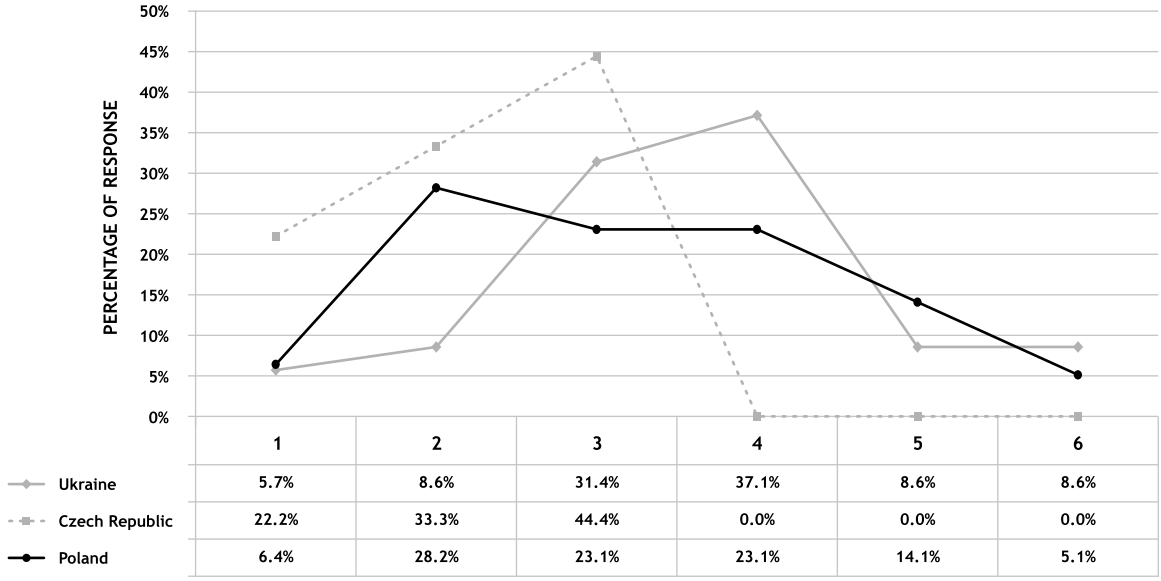
	1	2	3	4	5	6
Ukraine	8.6%	14.3%	17.1%	14.3%	25.7%	20.0%
Czech Republic	33.3%	33.3%	22.2%	11.1%	0.0%	0.0%
Poland	17.9%	28.2%	21.8%	17.9%	7.7%	6.4%

Figure 4. Results for the „Excessive talkativeness" factor
Source: own elaboration

quarter of the respondents from Poland completely ignored this factor, while scores given by the respondents from the Czech Republic fluctuated but were closer to the average.

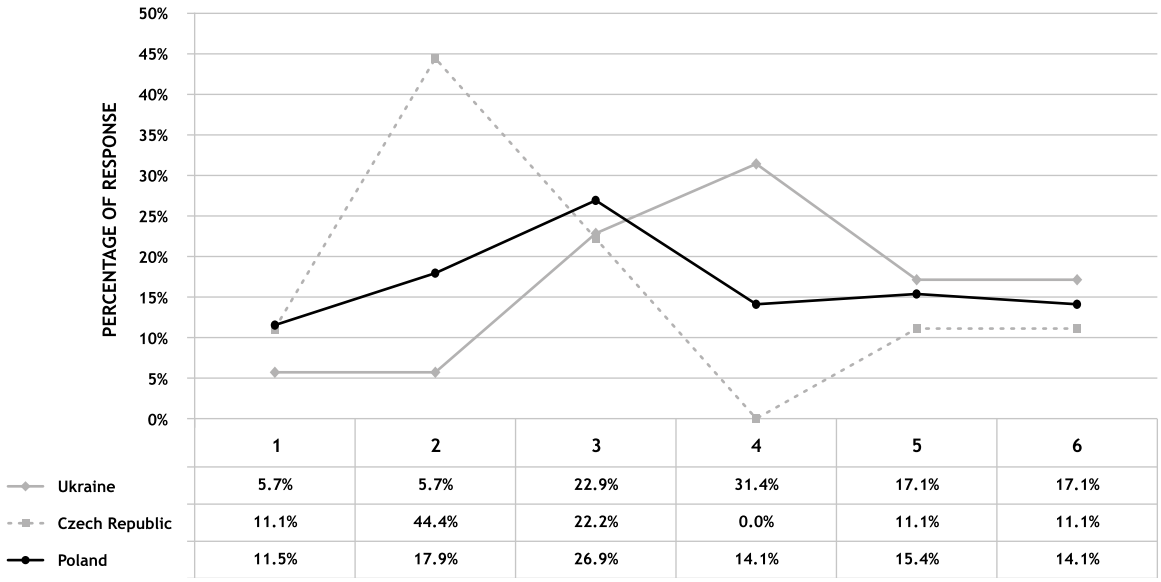
The second factor, „Rush and fatigue" (Figure 2), is more important to information security, according to the respondents. Almost half of the responses from Czech universities gave it an importance score of 5, and 40% of Ukrainian universities gave it a score of 4. In Poland, 30% of the respondents gave it the maximum rating, which was a score of 6. In the case of universities in each of the countries surveyed, the lowest scores given were 1 and 2.

The problem of excessive trust in third parties is assessed in a similar way across countries (Figure 3). In the case of the Czech Republic, we can observe a serious attitude to this particular problem. The highest number of the respondents gave scores of 3, 4 and 5; this accounted for 77.7% of the responses. Similarly, in Poland, 66.6% of the respondents from individual universities gave scores of 3, 4 and 5. The respondents from Ukraine are slightly less sensitive to this factor. Admittedly, 62.8% of the respondents gave scores of 3, 4 and 5, which is also a high result. Nevertheless, Ukraine also has the highest percentage of the respondents among the countries surveyed who consider this factor to be of little importance.



	1	2	3	4	5	6
Ukraine	5.7%	8.6%	31.4%	37.1%	8.6%	8.6%
Czech Republic	22.2%	33.3%	44.4%	0.0%	0.0%	0.0%
Poland	6.4%	28.2%	23.1%	23.1%	14.1%	5.1%

Figure 5. Results for the factor „Susceptibility to social engineering activities"
Source: own elaboration



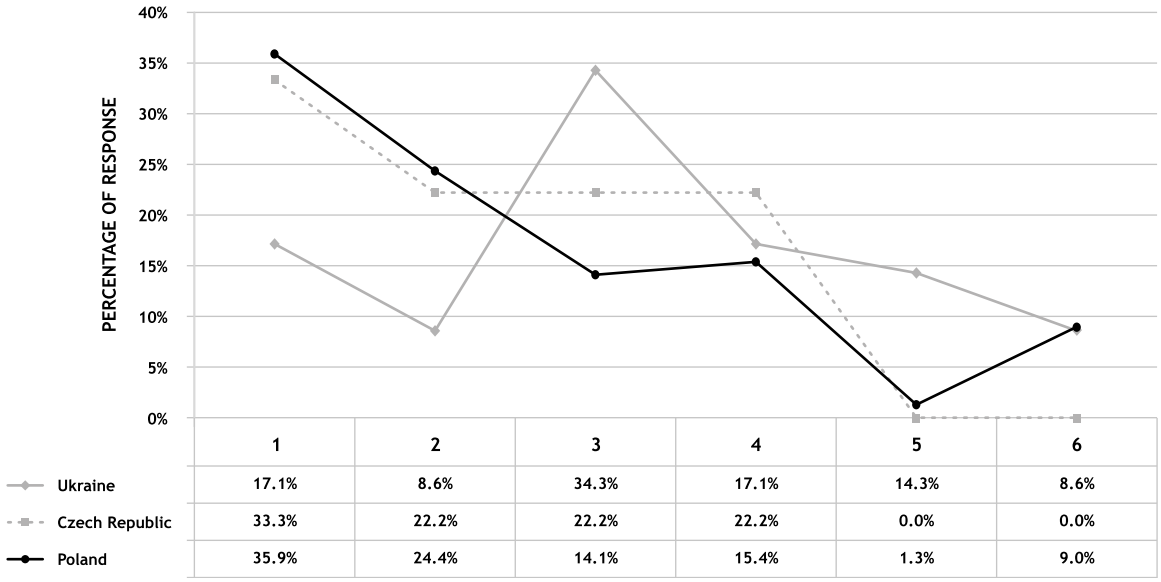
	1	2	3	4	5	6
Ukraine	5.7%	5.7%	22.9%	31.4%	17.1%	17.1%
Czech Republic	11.1%	44.4%	22.2%	0.0%	11.1%	11.1%
Poland	11.5%	17.9%	26.9%	14.1%	15.4%	14.1%

Figure 6. Results for the factor „Dissatisfaction with generally accepted working conditions"
Source: own elaboration

The fourth factor, „Excessive talkativeness" (Figure 4), is perceived differently in the countries surveyed. In Poland and the Czech Republic, this factor seems to be of little importance. 46.1% and 66.6% of the respondents from these countries gave it a score of 1 or 2 on the 6-point Likert scale. On the other hand, at Ukrainian universities, only 22.9% of the respondents gave it a score of 1 or 2, while as many as 45.7% of them gave it a score of 5 or 6.

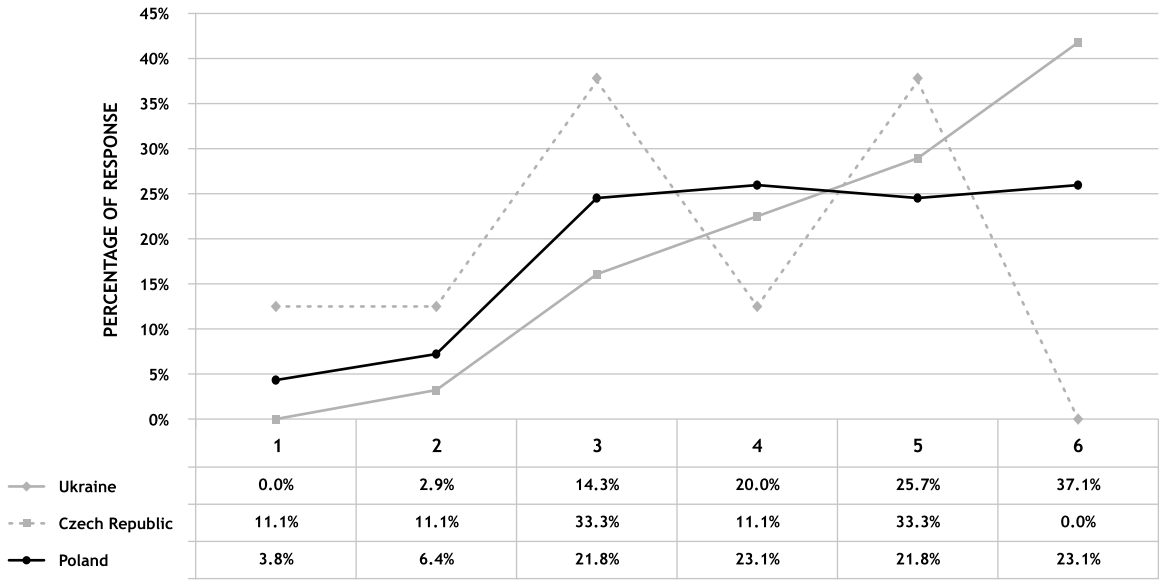
Quite surprising results were obtained for the „Susceptibility to social engineering activities" factor (Figure 5). Only 19.2% of the respondents in Poland, 17.2% of the respondents in Ukraine and no respondents in the Czech Republic gave it a score of 5 or 6 on the 6-point Likert scale. The results are surprising: according to a number of contemporary publications (BIK S.A., 2023; Fadhil, 2023; Farid et al., 2023; Kaczmarek, 2023; Ministerstwo Cyfryzacji, 2023; Pharris, Perez-Mira, 2022; Steinmetz, 2023), it is social engineering activities using phishing or vishing methods etc. that are the most dangerous and, at the same time, the most effective in phishing processes. These results certainly require further scientific inquiry and research.

Another factor, „Dissatisfaction with generally accepted working conditions", is perceived slightly differently from one country to another (Figure 6). In Poland, the



	1	2	3	4	5	6
Ukraine	17.1%	8.6%	34.3%	17.1%	14.3%	8.6%
Czech Republic	33.3%	22.2%	22.2%	22.2%	0.0%	0.0%
Poland	35.9%	24.4%	14.1%	15.4%	1.3%	9.0%

Figure 7. Results for the factor „Deliberate actions supported by a competing university (economic espionage)"
Source: own elaboration



	1	2	3	4	5	6
Ukraine	0.0%	2.9%	14.3%	20.0%	25.7%	37.1%
Czech Republic	11.1%	11.1%	33.3%	11.1%	33.3%	0.0%
Poland	3.8%	6.4%	21.8%	23.1%	21.8%	23.1%

Figure 8. Results for the factor „Lack of sufficient knowledge of information protection rules"
Source: own elaboration

percentage of the respondents giving minimum or lower scores (1,2,3) and higher or maximum scores (4,5,6) is similar: 56.3% and 43.7%, with 29.4% of them giving a score of 1 or 2 and 29.5% of them giving a score of 5 and 6. Therefore, we can conclude that the influence of this factor according to the respondents is moderate. However, the situation is different in Ukraine and the Czech Republic. In Ukraine, this factor is treated as a serious one. Scores of 4,5,6 on the 6-point Likert scale were given by 65.6% of the respondents. On the other hand, in the Czech Republic, this factor is considered to be of little importance. Scores of 1,2,3 on the 6-point Likert scale were given by 77.7% of the respondents.

The response to another factor, economic espionage, was also slightly different in the countries studied. In Poland and the Czech Republic, the majority of scores are the lower end of the scale (Figure 7). In Ukraine, there is not much difference between lowest and highest scores given, with most respondents giving scores 3 or 4. This may indicate a tendency towards centralised errors or indecision as to the importance of this factor.

The last of the surveyed factors, concerning the lack of knowledge in the field of information security, is considered very important by the respondents from two countries, while the respondents from one country consider it moderate (Figure 8). The vast majority of the respondents from Poland and Ukraine put their responses towards the top of the Likert scale. The highest number of scores of 4,5 or 6 was given by Ukrainian universities (82.8%), followed by Polish universities (68%) and Czech universities (44.4%). Thus, Czech universities have a rather balanced view of the contribution of this factor to the security of information resources.

Conclusion

In the modern reality of digital information processing, the impact of the human factor on information security is indisputable. Moreover, marketing departments of universities that manage information resources must comply with certain rules to ensure maximum protection for the intangible resources of their alma mater. The research presented in the article shows that people who manage information for the purpose of promoting their university also consider human factors to be important from the point of view of information security. The factors that have the greatest impact on the security of information resources are (taking into account the average values from all countries) are „Rush and fatigue" and „Lack of sufficient knowledge in the field of information protection rules", while the least significant factors are: „Deliberate actions supported by a competing university (economic espionage)" and „Uniformity of performed duties". On the other hand, an analysis of universities from individual countries indicates that the most influential factors in Poland coincide with average scores, while the least influential are „Deliberate actions supported by a competing university (Economic espionage)" and „Excessive talkativeness". In Ukraine, the most relevant factors also coincide with average scores plus the „Excessive trust in third parties" factor, while the least important factors also coincide with average scores. In the Czech Republic, the most important factors are: „Rush and fatigue" and „Excessive trust in third parties", while the least important are: „Excessive talkativeness" and „Susceptibility to social engineering".

This research may serve as a guideline for individual groups of universities in individual countries on how to conduct training and other activities aimed at eliminating possible vulnerabilities to potential human factors. They also provide a basis for continuing scientific investigations into information security at universities.

Paweł Kobis, Ph.D., D.Sc., Eng.
Czestochowa University of Technology
Faculty of Management
ORCID: 0000-0003-0714-1888
e-mail: pawel.kobis@pcz.pl

Artur Kisiołek, Ph.D., D.Sc., Eng.
Greater Poland Academy of Social and Economic Sciences in Środa Wielkopolska — Academy of Applied Sciences
Faculty of Economics
ORCID: 0000-0002-8815-6776
e-mail: a.kisiolek@wase.edu.pl

Prof., D.Sc. Oleh Karyy
Lviv Polytechnic National University, Ukraine
Department of Management of Organizations
ORCID: 0000-0002-1305-3043
e-mail: oleh.i.karyi@lpnu.ua

Doc. Ing. Adam Pawliczek, Ph.D., associate professor
Moravian Business College Olomouc, Czech Republic
Department of Management
ORCID: 0000-0001-7866-4972
e-mail: adam.pawliczek@mvso.cz

References

[1] Alavi R., Islam S., Jahankhani H., Al-Nemrat A. (2013), *Analyzing Human Factors for an Effective Information Security Management System*, „International Journal of Secure Software Engineering", Vol. 4, No. 1, pp. 50–74.

[2] Ani U. D., He H., Tiwari A. (2019), *Human Factor Security: Evaluating the Cybersecurity Capacity of the Industrial Workforce*, „Journal of Systems and Information Technology", Vol. 21, No. 1, pp. 2–35.

[3] APA PsycNET (2020), Publication manual of the American Psychological Association, 7th Ed, American Psychological Association, Washington.
[4] BIK S. A. (2023), Raport Antyfraudowy BIK 2023, https://rozwiazania-antyfraudowe.bik.pl/raporty/2023, data dostępu: 17.12.2023 r.
[5] Brzeziński A. (2023), *Specificity of Decentralized Autonomous Organizations as the Implementation of Blockchain Technology*, „Procedia Computer Science", Vol. 225, pp. 4371–4380.
[6] Ciekanowski Z., Rejman K., Szymański Z., Wyrębek H. (2017), *Zagrożenia cybernetyczne we współczesnym świecie*, „Przedsiębiorczość i Zarządzanie", Vol. 18, Nr 10, część 2, s. 43–56.
[7] Czernecka M., Szabuniewicz E., Zamorski P., Chabińska-Rossakowska M., Borzeszkowska A., Szefler A., Hyla M., Stanoch E., Pakulska M., Osiecka B., Dąbrowska-Olbryś S., Borczyk A. (2017), *Praca, moc, energia w polskich firmach. Sześć obszarów, które wpływają na efektywność organizacji*, Human Power, Łódź, https://epale.ec.europa.eu/sites/default/files/humanpower_raport_pracamoc energia_czesc02.pdf, data dostępu: 20.10.2023 r.
[8] Fadhil H. (2023), *Social Engineering Attacks Techniques*, „International Journal of Management Science and Engineering Management", Vol. 03, pp. 18–20.
[9] Farid G., Warraich N. F., Iftikhar S. (2023), *Digital Information Security Management Policy in Academic Libraries: A Systematic Review (2010–2022)*, „Journal of Information Science", https://journals.sagepub.com/doi/10.1177/01655515231160026.
[10] Ghafir I., Saleem J., Hammoudeh M., Faour H., Prenosil V., Jaf S., Jabbar S., Baker T. (2018), *Security Threats to Critical Infrastructure: The Human Factor*, „The Journal of Supercomputing", Vol. 74, No. 10, pp. 4986–5002.
[11] Kaczmarek A. (2023), *Raport Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA) dotyczący zagrożeń dla bezpieczeństwa informacji z 2022 r.*, https://www.traple.pl/raport-europejskiej-agencji-ds-cyberbezpieczenstwa-enisa-dotyczacy-zagrozen-dla-bezpieczenstwa-informacji-z-2022-r/, data dostępu: 16.12.2023 r.
[12] Kobis P. (2021), *Zarządzanie bezpieczeństwem informacji w systemach informacyjnych małych i średnich przedsiębiorstw z uwzględnieniem czynnika ludzkiego*, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora", Toruń.
[13] Kobis P., Karyy O. (2021), *Impact of the Human Factor on the Security of Information Resources of Enterprises during the COVID-19 Pandemic*, „Polish Journal of Management Studies", Vol. 24, pp. 210–227.
[14] Kobis P., Kisiołek A. (2018), *Zarządzanie bezpieczeństwem danych w przedsiębiorstwach MSP z uwzględnieniem czynnika ludzkiego – wyniki badań*, „Przegląd Organizacji", Nr 8, s. 44–52.
[15] Kołodziejczyk E. (2017), *Monotonia pracy może być powodem znacznej uciążliwości psychicznej*, https://www.prawo.pl/kadry/monotonia-pracy,189329.html, data dostępu: 17.10.2023 r.
[16] Konarska M. (2003), *Monotonia jako czynnik obciążenia podczas pracy – ocena ryzyka zawodowego*, „Bezpieczeństwo Pracy: Nauka i Praktyka", Nr 3, s. 13–16.
[17] Ministerstwo Cyfryzacji (2023), Socjotechnika – dlaczego cyberprzestępcy są skuteczni? Portal Gov.pl, https://www.gov.pl/web/cyfryzacja/socjotechnika--dlaczego-cyberprzestepcy-sa-skuteczni, data dostępu: 16.12.2023 r.
[18] Mitnick K. D., Simon W. L. (2003), *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons, New York.
[19] Noga M., Brzeziński A. (2021), *Economics, Education and Youth Entrepreneurship: International Perspectives*, Routledge Taylor & Francis Group, London, New York.
[20] Pharris L., Perez-Mira B. (2022), *Preventing Social Engineering: a Phenomenological Inquiry*, „Information & Computer Security", Vol. 31, No. 1, pp. 1–31.
[21] Pufal P. (2014), *Czym jest gadulstwo*, https://artelis.pl/artykuly/59288/Czym-jest-gadulstwo, access date: 20.10.2023.
[22] Sedgwick S. (2019), *The Human Factor of Cyber Security*, https://www.csoonline.com/article/3504813/the-human-factor-of-cyber-security.html, access date: 15.12.2023.
[23] Sejm Rzeczypospolitej Polskiej (2019), ISAP – Internetowy System Aktów Prawnych, Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 16 maja 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Kodeks pracy, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190001040, data dostępu: 13.12.2023 r.
[24] Steinmetz K. F. (2023), *Executing Effective Social Engineering Penetration Tests: a Qualitative Analysis*, „Journal of Applied Security Research", Vol. 18, No. 2, pp. 246–266.
[25] Wielki słownik języka polskiego (2014), gadulstwo, https://wsjp.pl/index.php?id_hasla=47559, data dostepu: 10.12.2023 r.
[26] Żebrowski A. (2016), *Zagrożenia i bezpieczeństwo przemysłu zbrojeniowego u progu XXI wieku (wybrane aspekty)*, http://rep.up.krakow.pl/xmlui/handle/11716/3141, data dostępu: 14.10.2023 r.

Czynnik ludzki w bezpieczeństwie zasobów informacyjnych działów marketingu uczelni wyższych w Polsce, Ukrainie i Republice Czeskiej

Streszczenie

Celem artykułu jest prezentacja wyników badań dotyczących postrzegania przez pracowników działów marketingu uczelni wyższych w Polsce, Ukrainie i Republice Czeskiej stopnia zagrożenia dla bezpieczeństwa zasobów informacyjnych wynikającego z czynników ludzkich. Wyszczególniono i opisano w części teoretycznej artykułu najczęściej występujące w literaturze przedmiotu czynniki wywodzące się z zachowania, cech, kompetencji pracowników i mające wpływ na bezpieczeństwo zarządzania informacją. W części empirycznej zaprezentowano wyniki badań przeprowadzonych w Polsce, Ukrainie i Republice Czeskiej w okresie od listopada 2021 roku do czerwca 2023 roku.

Słowa kluczowe

bezpieczeństwo informacji, czynnik ludzki, e-marketing, uczelnie wyższe