THREATS TO INFORMATION SECURITY DRIVEN BY HUMAN FACTOR IN THE PERCEPTION OF PERSONS IN CHARGE OF INTANGIBLE RESOURCES MANAGEMENT

DOI: 10.33141/po.2021.5.03

Organization Review, No. 5(976), 2021, pp. 19-27

www.przegladorganizacji.pl

Paweł Kobis, Artur Kisiołek, Oleh Karyy, Grzegorz Chmielarz

Introduction

Information security management in enterprises can be analysed with regard to many aspects. This is largely driven by the nature of cognitive ideas (data, information, knowledge), which currently are mostly stored on digital carriers, but also in the paper form, sound recordings, videos, and in the form of knowledge and experience of employees. Managing security of intangible resources in so many dimensions requires involvement of persons whose responsibilities are limited exclusively to ensuring the security of the abovementioned resources. In practice, these are IT departments, individual IT staff members (digital resources), and Data Protection Officers. Apart from employing persons to be in charge of protecting data and information in economic entities, it is equally necessary to implement indispensable law regulations, rules of conduct, instructions in the form of security policies. It is also necessary to implement a system of training that guarantees provision of up-to-date and essential knowledge to employees, which will support them in everyday management of information resources.

Managing properly information security in micro and small enterprises is of particular significance. In these entities human capital and financial resources are limited, and as a consequence, they do not maintain their own IT departments. Some of them (micro enterprises in particular) do not even employ staff members responsible exclusively for ensuring the security of the information managed by a given entity (KPMG, 2020; Deloitte Access Economics, 2016). Therefore, protection of intangible resources rests entirely on those employees or persons who are in charge of information security only through extra responsibilities.

The subject of the article is the presentation of selected aspects related to the human factor, that is all behaviours and conduct of employees in the course of information management process, being a sum of their competencies, psychophysical condition, and frequently own intensions. We have attempted to determine their influence on generating threats while using popular software solutions. The underlying objective of the article is to present the role of the human

factor in generating potential threats to security of intangible resources while using selected application solutions, and its perception by enterprise employees confronted with technical security systems.

For the purpose of this publication, we present the results of the research conducted in 2020 in a group of micro and small enterprises. The objective of the research was to investigate the awareness of persons who manage information and their perception of the impact of the human factor on threats to intangible resources security. While conducting the research, we focused on mistakes that employees make while using basic computer software owned by the majority of economic entities: electronic mail, office software, Internet browser and other solutions essential in everyday work consisting in processing of information resources. Thus, the discussions and studies presented in the paper, pertaining to the human factor, have been analysed by us through the prism of data and information in the digital form, managed with the use of the abovementioned software.

Selected theoretical aspects pertaining to impact of human factor on information security

Presently, security of information resources can be analysed in two dimensions:

- technical and organisational one;
- behavioural one.

Technical and organisational dimension of information security pertains to all the activities in the areas of:

- hardware and software;
- applicable legal standards in force;
- internal regulations that normalise manners of information management.

Information security in the technical and organisational aspect is commonly understood in enterprises and implemented at various, individually perceived levels of security. Individual perception can be defined here as a specific, resulting among others from the competencies, attitude of a particular person or persons to information security. The individual attitude also results from particular requirements of security, e.g. sensitive information may exist in an enterprise, and it requires special protection. It involves financial capabilities with regard to purchases of hardware, software, technologies for information protection, and the IT model functioning in the organisation. Each model (traditional, cloud computing) generates a different attitude to intangible resources security.

In the case of behavioural dimension, information security is still analysed only in the limited scope in scientific and popular literature alike. The subject in the aspect of information security in the behavioural dimension is man, and all the vulnerabilities of the information system and threats to information are analysed through so called the human factor (Kobis, Kisiołek, 2018, p. 45). The term „human factor" has been defined over the years in the literature in a number of ways (DeMarco, Lister, 2002; Grudzewski et al., 2001; Jamka, 2011; Koźmiński, Jemielniak, 2008; Mikuła, 2003; Olejniczuk-Merta, 2015), also depending on the scientific discipline in which the issues have been analysed and context of deliberations related to human activity (Fellner, Osowski, 2015; Kałużna, Fellner, 2014). In the present paper, the notion of the human factor has been based on the definition by Y. Wanga (2008, p. 75), who writes that: „*human factors are the roles and results of human activity in the system, which introduce additional strengths, weaknesses and uncertainties*". The author of the definition also specifies the taxonomy of human factors, in which he details factors in a breakdown into the three distinguished in the definition categories (Table 1).

The factors that have been included in Table 1 result both from the human nature itself – the personality, disposition, natural behaviours, inclinations as well as competencies. In the case of competencies, the ones that directly concern employees (Oleksyn, 2018, p. 33) are:

- psychophysical features;
- internal motivation;
- health condition;
- abilities;
- predispositions;
- attitudes and behaviours;
- rights to take actions;
- skills;
- experience;
- knowledge;
- education.

The presented competencies directly impact the manner of information management by employees. This concerns both the substantial aspect of information processing as well as the aspect of secure information management. Contemporary attacks on IT systems of enterprises in most cases exploit man as the weakest link of the security system. They rely on possible errors, negligence of employees who make them and so allow the attacker to bypass, frequently complex, protective measures of the IT system (Kobis, 2021, pp. 165–166).

Table 1. Taxonomy of human factors

Category	Factors
strengths	natural intelligence, autonomous behaviours, complex process of making decisions, highly-qualified actions, intelligent senses, strength of perception, complicated human coordination, ability to adapt
weaknesses	low efficiency, slow reactions, error prone, tiredness, concentration loss
uncertainties	productivity, accuracy, reaction time, perseverance, reliability, attitude, execution, motivation to try uncertain actions

Source: Wang, 2008, p. 75

Man's actions in the realm of threats to information may take various forms. They can include, among others, opening attachments to electronic mail without having become acquainted with its content beforehand or executing files of unknown origin. Other examples of bad behaviours are installing untested software from the Internet or keeping passwords and other confidential data on so called „yellow cards", which are usually stuck to the monitor or desk. There is also vulnerability to social engineering from attackers who want to obtain access to information and spying. Each of the listed employee behaviours may lead to loss or damage to information, and consequently, cause financial losses for the economic entity, loss of its reputation, and even bankruptcy, in a situation when the information revealed is of key importance for the enterprise's operations.

In the empirical part of the paper, we have distinguished five most frequently cited in the literature factors that impact man's behaviour in everyday processing of intangible resources: negligence, curiosity, carelessness, haste and tiredness as well as lack of knowledge (Dykstra, Paul, 2018; Górski, Wojsa, 2018, p. 44; Sobolewska, 2018, p. 118). These are the factors that impact the generation of potential threats, defined as unintentional and resulting from employees' predispositions themselves. Their brief characteristics have been presented below.

Negligence is defined as the lack of diligence in something, carelessness (Słownik Języka Polskiego PWN, 2021b). This concerns employees who intentionally or unconsciously do not comply with essential principles of information protection, doing so out of their own convenience (e.g. setting weak access passwords), laziness, attempt to save time (e.g. not logging out of the system while leaving their work post).

Curiosity in turn is defined as a compulsive urge to learn „something", against the existent, commonly accepted rules. Examples of such a behaviour may include: opening email attachments from senders that they are unable to identify, or visiting Internet websites classified as „dangerous" ones.

Carelessness defines employees who are unaware of the consequences of their own deeds or taking particular actions without further thoughts (Słownik Języka Polskiego PWN, 2021a). This is the factor that is frequently exploited in social engineering by potential aggressors. Persons being subject to social engineering techniques and simultaneously characterised by carelessness become tools in the hands of hackers, making it possible for them to acquire or destroy particular information resources. The most frequently used IT tools in this respect include: electronic mail, instant messaging, prepared website (Aldawood et al., 2020, pp. 45–49; Exclusive Networks, 2019; Cisco, 2019, p. 6).

Another factor, haste and tiredness, may concern practically every employee and so it poses a particularly serious threat. In everyday functioning of enterprises, one can frequently observe a number of situations where something is done „ASAP". The need for specific tasks to be carried out instantly causes that details remain overlooked. Moreover, excess of such situations leads to tiredness – another factor that decreases the level of employees' concentration. As a consequence, a situation may occur when employees install software having not checked carefully its origin, open subsequent email messages without analysing their content, seek for information online without paying attention to websites they visit, etc.

The last of the described factors is the lack of knowledge. This is the key factor that needs to be verified already at the stage of recruiting employees, and then appropriately eliminated. The most effective tool to eliminate this factor is cyclical training, internal or external one, creation of an internal database that can be accessed by all the employees.

It is difficult to attribute unequivocally the determined human factors to particular actions of employees that may pose a threat to information. It can be stated that it is highly probable that the majority of actions that are potentially threatening to intangible resources is a sum, resultant of all the abovementioned factors. They are also used in attacks based on social engineering techniques. Susceptibility of employees to particular techniques often derives from the enumerated factors. Therefore, hackers attempt to make use of all the vulnerabilities driven by human nature so as to acquire or destroy particular information resources.

While analysing the literature on the subject, one can conclude that these days the human factor is recognised to be one of the main reasons for information loss in the case of economic entities. For example, the report published by Tessian (2021) „The Psychology of Human Error", presents the results of the research conducted among 2000 employees in the USA and Great Britain. The results show that as many as 88% of cases of compromising information security result from human errors. Moreover, the same research (Tessian, 2021, p. 5) shows that:

- 58% of employees have sent an email to the wrong person at work;
- 57% of employees are more distracted when working from home;
- 43% of people have made mistakes at work that compromised cybersecurity;
- younger workers are 5 times more likely to make mistakes with security consequences;
- over half of employees make more mistakes when they are stressed, while 43% are more error-prone when tired;
- 93% of staff are tired and stressed at work;
- 1 in 10 feel tired every day of the week;
- a third of workers rarely or never think about cybersecurity at work.

The cited results are deeply disturbing, and they confirm that today man and his behaviour, stemming from particular human factors, is the most threatening thing for information security. In the empirical part of the paper, we have demonstrated how such factors as: negligence, curiosity, carelessness, haste and tiredness as well as the lack of knowledge are perceived to be threats to intangible resources security among employees of enterprises from the Silesian province in Poland.

Research method

The research was carried out in the period from July to November 2020 in micro and small enterprises

registered in the territory of the Silesian province. The survey questionnaire included in total 8 questions pertaining to information security and was conducted with the use of the CAWI (Computer Assisted Web Interview) method. The survey participants were the persons who process information (office employees). For the purpose of the present paper we have presented 2 out of 8 obtained results of the research.

In the selection of enterprises, we applied the purposeful selection, distinguishing these entities that in their everyday operations use office software, electronic mail, and other applications to process information resources. We have assumed that software of this type is used by the majority of economic entities, and processing information in these applications is most vulnerable to potential threats caused by human error.

The number of enterprises indispensable for the research was determined based on the dependence (Biostat, Centrum Badawczo-Rozwojowe, 2021):

$$N_{min} = \frac{P(1-P)}{\frac{e^2}{z^2} + \frac{P(1-P)}{N}}$$

Where:

N_{min} – minimum research sample – the smallest possible number of enterprises to conduct the research;

N – size of total population;

e – maximum assessment error;

z – value resulting from the adopted trust level (α), calculated with the use of distribution function of standard distribution. For 95% trust level z=1.96;

P – estimated fraction size (in the research 0.7 has been assumed, on an assumption that the investigated feature occurs in 70% of the population).

In the research we adopted the value N=231 467 (224 518 of micro enterprises and 6949 of small ones). This is the number of non-financed micro and small enterprises according to the Main Statistical Office for the year 2018 in the Silesian province. In the breakdown of enterprises, we considered the number of employees (1–9 employees are micro enterprises and 10–49 employees are small ones). The data does not cover: entities conducting activity classified according to the Polish Classification of Activity of 2007 into section A (Agriculture, Forestry, Hunting and Fishery), K (Financial and Insurance Activity), and O (Public Administration and National Defence, Compulsory Social Security) (GUS, 2020). The calculations we did showed that the required number of enterprises to participate in the research was 322. Therefore, the research was conducted in the group of 354 enterprises, which included 278 micro ones and 76 small ones, which complies with the calculated requirement. The survey participants included service, manufacturing entities, traders, and those of mixed profile of activity (Table 2).

Research results

The first question to the respondents was about the perception of information security in a given economic entity. For this purpose, the respondents were asked to evaluate on the 5-point scale (Likert scale) to what extent information security is impacted by technical measures, and how it is conditioned by the conduct of persons in charge of information security. The distribution of the respondents' answers has been presented in Figure 1. The answers demonstrate that the respondents recognise technical measures to ensure a higher level of security. The conduct of those who process intangible resources is less relevant. In the case of the top indication (5), the percentage ratio of the indications to technical measures compared to the human factor is as much as 48.02% to 7.91%. In the case of 4-point indications, the same relation is 51.41% to 40.68%. Therefore, as many as 99.43% of the respondents indicated top values of the scale, that is 4 and 5. In the same range of the scale, the human factor was selected by less than a half of the investigated respondents – 48.59%, while as many as 39.83% of the respondents selected the value 3 and 11.58% of them selected the value of 2.

The second question of the survey was about the human factor itself. For this purpose, we distinguished 5 factors most frequently cited in the literature on the subject and believed to contribute to man's mistakes while managing information. The respondents were asked to express their opinions, based on their knowledge and beliefs, about the given factor's impact on the following behaviours: opening electronic mail attachments, opening files of unknown origin, installing untested software from the Internet by users of computers and mobile devices. The evaluation was conducted with the use of the 5-point scale. It needs to be mentioned that in the literature on the subject these are considered to be the most frequently made mistakes posing a threat to information resources. In Table 3, we have summarised the results of the average, median, and dominant for each of the factors in a breakdown into the size of enterprises.

Table 2. Breakdown of investigated enterprises into the type of conducted activity

	Micro enterprises (n=278)	Small enterprises (n=76)	Total enterprises (n=354)
services	153	28	181
manufacturing	42	19	61
trade	37	11	48
mixed	46	18	64

Source: own analysis

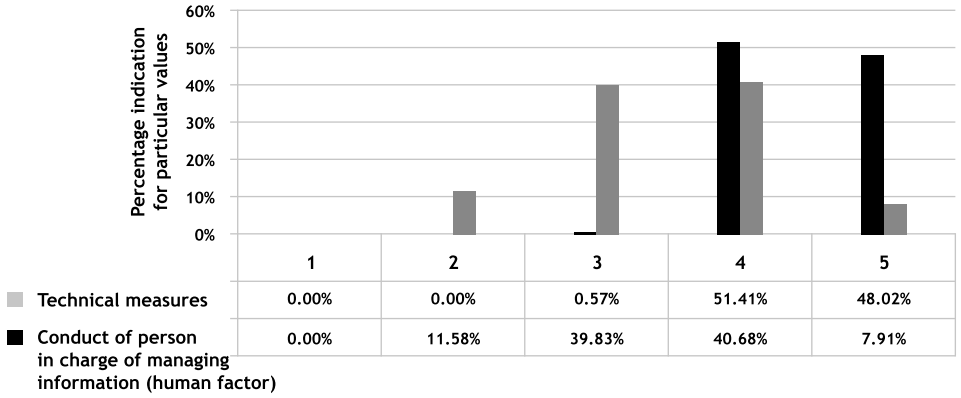


Figure 1. Dependence of information security on technical measures vs human factor – comparison of respondents' answers. Percentage level of indications of particular values on the Likert scale from 1 to 5
Source: own analysis

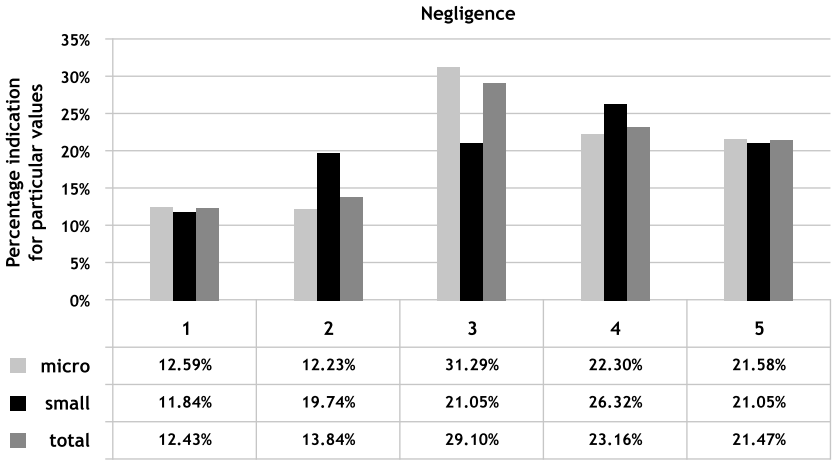


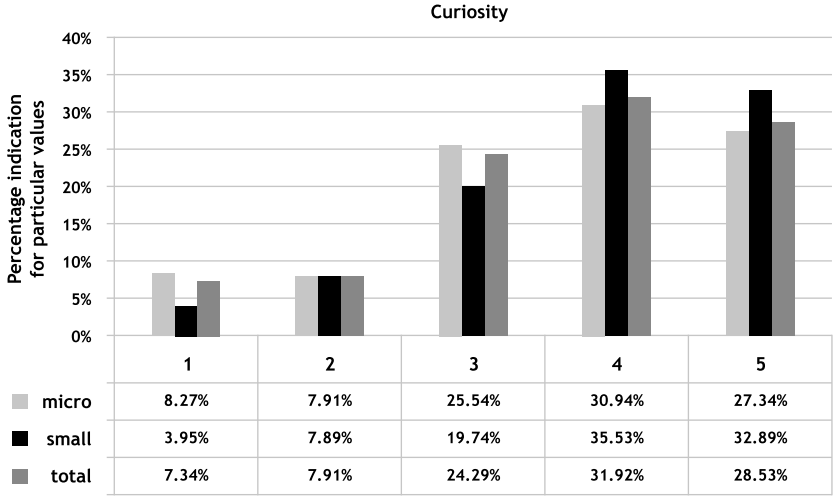
Figure 2. Negligence and its impact on undesirable actions: opening email attachments, opening files of unknown origin, installing untested software from the Internet. Percentage level of indications of particular values on the Likert scale from 1 to 5
Source: own analysis

Table 3. Median and dominant results for individual respondents' indications

	Respondents' answers to the question: „What can be the reasons for the following undesirable actions: opening attachments to electronic mail, opening files of unknown origin, installing untested software from the Internet? (Please select answers on the scale from 1 to 5, where 1 means minimum significance and 5 maximum one)"					
	Micro enterprises (n=278)		Small enterprises (n=76)		Total enterprises (n=354)	
	median	dominant	median	dominant	median	dominant
negligence	3	3	3	4	3	3
curiosity	4	4	4	4	4	4
carelessness	4	4	4	4	4	4
haste and tiredness	3	3	4	4	3	3
lack of knowledge	4	5	4	4	4	5

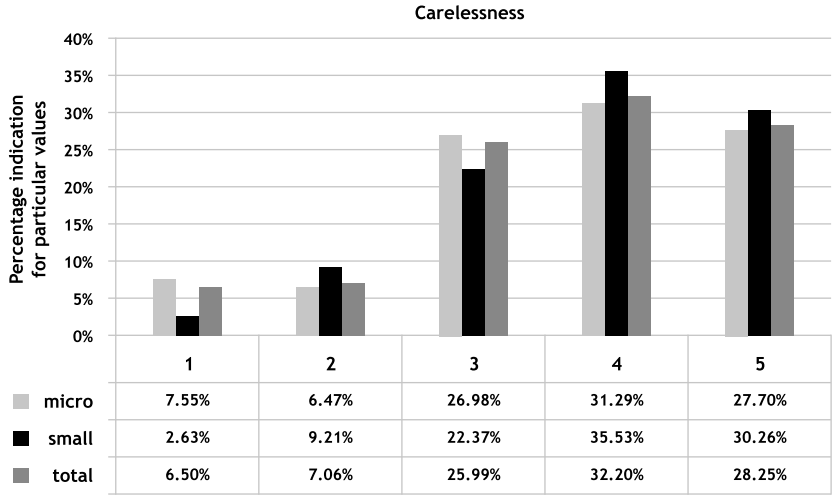
Source: own analysis

The results of respondents' indications for the first factor, negligence, have been presented in Figure 2. The curves demonstrate the percentage number of indications for particular values from 1 to 5 in a breakdown into micro and small enterprises. In the case of micro enterprises, 3 was the value that received the greatest number of indications. This may prove that the respondents treat negligence as the factor of average importance for information security. The results might have also been affected by so-called central tendency error. In the case of small entities, the greatest number of indications received the value of 4 – this factor was more „appreciated" by the respondents. While analysing the answers given by all the enterprises participating in the research, one can conclude that a greater number of respondents selected the values from the upper range of the scale (from 3 to 5).



	1	2	3	4	5
micro	8.27%	7.91%	25.54%	30.94%	27.34%
small	3.95%	7.89%	19.74%	35.53%	32.89%
total	7.34%	7.91%	24.29%	31.92%	28.53%

Figure 3. Curiosity and its impact on undesirable actions: opening email attachments, opening files of unknown origin, installing untested software from the Internet. Percentage level of indications of particular values on the Likert scale from 1 to 5
Source: own analysis



	1	2	3	4	5
micro	7.55%	6.47%	26.98%	31.29%	27.70%
small	2.63%	9.21%	22.37%	35.53%	30.26%
total	6.50%	7.06%	25.99%	32.20%	28.25%

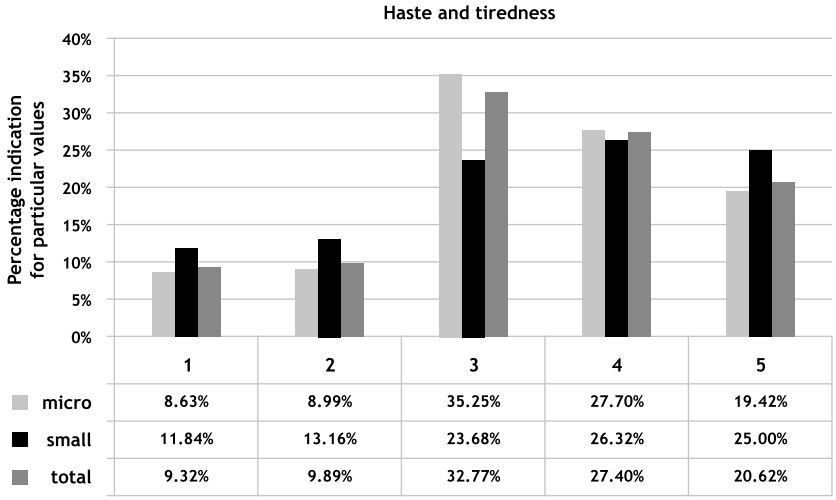
Figure 4. Carelessness and its impact on undesirable actions: opening email attachments, opening files of unknown origin, installing untested software from the Internet. Percentage level of indications of particular values on the Likert scale from 1 to 5
Source: own analysis

Another investigated factor was „curiosity". While analysing the indications presented in Figure 3, one can state that in the opinion of the respondents this factor to a larger extent than "negligence" impacts improper behaviours of employees with respect to their processing of information resources. Greater percentage indications can be observed for the values of 4 and 5 (respectively 30.94% and 27.34% for micro enterprises, 35.53% and 32.89% for small ones). In comparison with negligence, a smaller number of the respondents underestimate the significance of „curiosity" (8.27% of micro enterprises and only 3.95% of small ones for the indication equal to 1).

For the factor „carelessness" the results of the research are similar to those for „curiosity". One can observe it while analysing the shapes of the curves. They are similar and reflect similar percentage indications for particular values from 1 to 5. While analysing the notions themselves, a conclusion can be put forward that excessive curiosity of employees may lead to careless, inconsiderate actions.

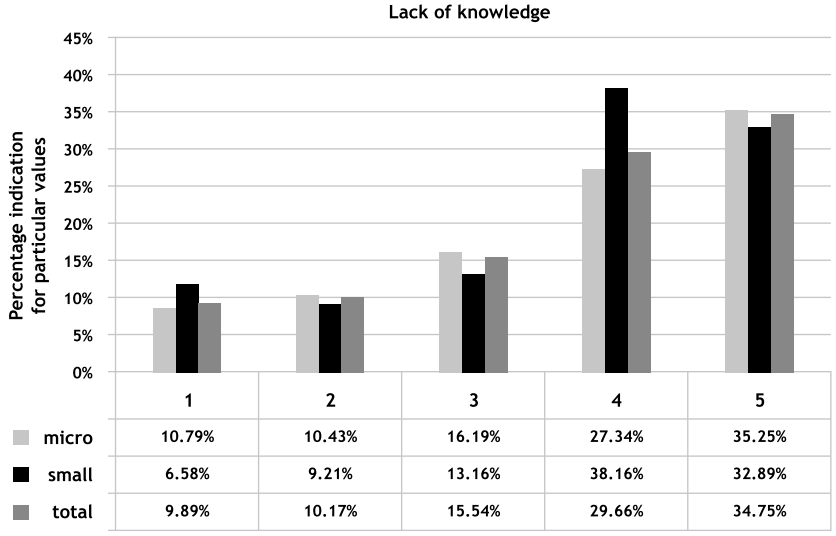
Another factor we investigated was „haste and tiredness" (Figure 5). In this case most of the respondents selected the third answer, which can be termed as the most „universal one". To a certain extent, this can reflect uncertainty of the survey participants as to the impact of this factor on information security. This can also stem from the respondents' unwillingness to admit that this factor occurs at their workplace – this could prove that they have been assigned too many responsibilities or they lack proper training necessary to render work at this workplace. Considering all the investigated economic entities, only 9.32% of the respondents recognise this factor as insignificant (indications of 1), but twice as many of them believe it to be particularly important (indications of 5).

The last factor we investigated was „lack of knowledge" (Figure 6). Knowledge as one of the employee competencies (Oleksyn, 2018, p. 33) is of key importance in the processes of proper management of information resources. Moreover, this knowledge has to be as up-to-date as possible. It should be acquired not only in educational processes, but also in the



	1	2	3	4	5
micro	8.63%	8.99%	35.25%	27.70%	19.42%
small	11.84%	13.16%	23.68%	26.32%	25.00%
total	9.32%	9.89%	32.77%	27.40%	20.62%

Figure 5. Haste and tiredness and its impact on undesirable actions: opening email attachments, opening files of unknown origin, installing untested software from the Internet. Percentage level of indications of particular values on the Likert scale from 1 to 5
Source: own analysis



	1	2	3	4	5
micro	10.79%	10.43%	16.19%	27.34%	35.25%
small	6.58%	9.21%	13.16%	38.16%	32.89%
total	9.89%	10.17%	15.54%	29.66%	34.75%

Figure 6. Lack of knowledge and its impact on undesirable actions: opening email attachments, opening files of unknown origin, installing untested software from the Internet. Percentage level of indications of particular values on the Likert scale from 1 to 5
Source: own analysis

processes of continuous training, becoming acquainted with new techniques, technologies related both to solutions applied in the area of information management as well as newly-emerging threats, means of illegal information acquisition. This is the key factor that allows to recognise and eliminate a threat. While analysing the data presented in Figure 6, one can observe that as many as 62.59% of the respondents consider this factor to be either important (4) or particularly important (5). It can be assumed that employees are aware of the impact of proper knowledge on information security.

Discussion

The research conducted among micro and small enterprises in the Silesian province allows for formulation of two primary conclusions:

- employees believe that technical (hardware and software) measures are more important than the conduct of persons processing information, in the context of intangible resources security;
- the investigated human factors are in the opinion of the respondents significant from the perspective of information security.

As the research results presented in Figure 1 demonstrate, the human factor is still not perceived by employees as the most essential one in the process of information security. The word „still" has been used here deliberately. The fact is, that all the research conducted by the largest investigation agencies and scientific publications indicate that improper conduct of employees (intentional, unintentional, and resulting from psychophysical features) poses the most serious threat to information security (Bada et al., 2019; Dreyer et al., 2018; Exclusive Networks, 2019). All the attacks that aim to obtain information fraudulently or destroy it, such as phishing or ransomware, make us of social engineering, treating man as the weakest link

of the security system. No technical measures (hardware and software) will operate properly if persons using them intentionally or unintentionally allow or accept particular connections, open files of unknown origin, install software coming from unknown sources, or are careless while browsing websites.

Despite the fact that the respondents indicated the technical factor as the prevailing one in the aspect of information security, they are also aware of the role employees play in this process. This is confirmed by the research results presented in Figures 2–6. Each of the investigated factors received more indications for the values of 4 and 5 than for the values of 1 and 2. Therefore, each of them was recognised as a significant one and having impact on generation of potential threats to intangible resources. The results also demonstrate subtle differences between the respondents representing micro and small enterprises. The employees of small enterprises more frequently selected the answers 4 and 5 than the ones working in micro ones. The disparities are not large (several percentage points). However, they prove greater awareness (and possibly experience) as to the threats resulting from employee behaviours, which can be an outcome of more intense training or qualifications of the employees themselves. Yet, this has not been proved in this research. Our research presented in the article is in line with all the research investigating human mistakes while managing information. Its results should motivate managerial staff members to attach greater importance to a widely understood human factors while securing information. These are more important than technical measures themselves, as they will not fulfil their role properly without qualified and trained employees.

Conclusion

The advancement level of contemporary information security systems allows for securing efficiently own intangible resources. The prerequisite for their proper functioning and fulfilling their role is appropriate oversight of persons trained to do so. However, even the most technically advanced measures will not protect information if access to these resources is consciously or unconsciously granted by humans themselves. Therefore, it is necessary to introduce particular corrective measures meant to eliminate the so-called „human factor" in the process of information security management. The necessary remedies include cyclical training, applying adequate recruitment procedures while selecting employees for a given position, ensuring proper working conditions for employees, increasing their awareness of the threats they can provoke themselves.

The subject matter of protecting appropriately a computer workplace with reference to the human factor is very extensive and it covers a wide range of aspects that have not been analysed in the present paper, e.g., sharing common hardware, the BYOD (Bring Your Own Device) trend, security policies, industrial espionage. Thus, the paper refers to part of a wide range of issues pertaining to the human factor in information security. It should also be stressed that the conducted research reflects the answers given with regard to using popular software solutions. Therefore, it cannot be referred to employee behaviours in all the activities related to information management. The remaining areas of employee behaviours may then constitute a continuation of the research presented in this article.

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

Artur Kisiołek, Ph.D., Eng.
The Greater Poland University of Social Sciences and Economics in Środa Wlkp.
Department of Economics
ORCID: 0000-0002-8815-6776
e-mail: a.kisiolek@wwsse.pl

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

Grzegorz Chmielarz, Ph.D.
Częstochowa University of Technology
Faculty of Management
ORCID: 0000-0002-1587-0733
e-mail: grzegorz.chmielarz@pcz.pl

References

[1] Aldawood H., Alashoor T., Skinner G. (2020), *Does Awareness of Social Engineering Make Employees More Secure?* „International Journal of Computer Applications", No. 177(38), pp. 45–49.

[2] Bada M., Sasse A.M., Nurse J.R.C. (2019), *Cyber Security Awareness Campaigns: Why do they Fail to Change Behaviour?* https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf, access date: 14.03.2021.

[3] Biostat, Centrum Badawczo-Rozwojowe (2021), *Kalkulator wielkości próby, teoria i przykłady*, https://www.statystyka.az.pl/dobor/kalkulator-wielkosci-proby.php, data dostępu: 14.04.2021 r.

[4] Cisco (2019), *Wiadomość e-mail: klikaj z ostrożnością. Jak się chronić przed phishingiem, oszustwem i innymi podstępami*, https://branden.biz/wp-content/uploads/ 2019/07/ email-threat-report-2019_Cisco.pdf, data dostępu: 17.04.2021 r.

[5] Deloitte Access Economics (2016), *Report: Connected Small Businesses 2016*, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/Economics/deloitte-au-economics--connected-small-businesses-google-051016.pdf, access date: 17.04.2021.
[6] DeMarco T., Lister T.R. (2002), *Czynnik ludzki: Skuteczne przedsięwzięcia i wydajne zespoły*, WNT, Warszawa.
[7] Dreyer P., Jones T., Klima K., Oberholtzer J., Strong A., Welburn J.W., Winkelman Z. (2018), *Estimating the Global Cost of Cyber Risk: Methodology and Examples*, Santa Monica, Calif.: RAND Corporation, RR-2299-WFHF, https://www.rand.org/pubs/research_reports/RR2299.html, access date: 11.03.2021.
[8] Dykstra J., Paul C.L. (2018), *Cyber Operations Stress Survey (COSS): Studying Fatigue, Frustration, and Cognitive Workload in Cybersecurity Operations*, Proceedings of the 11th USENIX Conference on Cyber Security Experimentation and Test, https://www.usenix.org/system/files/conference/cset18/cset18-paper-dykstra.pdf, access date: 17.04.2021.
[9] Exclusive Networks (2019), *Proofpoint – Human Factor Report 2019*, Exclusive Networks, Sweden, https://www.exclusive-networks.com/se/proofpoint-human-factor-report-2019/, access date: 14.04.2021.
[10] Fellner A., Osowski M. (2015), *Uwzględnienie czynnika ludzkiego w analizie bezpieczeństwa procesu zarządzania zasobami ludzkimi*, „Problemy Kryminalistyki", Nr 290, s. 35–45, 94–103.
[11] Górski G., Wojsa M. (2018), *Wybrane ataki mające na celu kompromitację danych poufnych oraz metody zapewnienia bezpieczeństwa aplikacji i usług internetowych*, „Zeszyty Naukowe Wydziału Elektroniki i Informatyki Politechniki Koszalińskiej", Nr 12, s. 35–48.
[12] Grudzewski W.M., Michałowska A., Rozenbajgier A. (2001), *Zarządzanie zasobami ludzkimi w XXI wieku*, „Ekonomika i Organizacja Przedsiębiorstwa", Nr 5, s. 3–10.
[13] GUS (2020), *Działalność przedsiębiorstw niefinansowych w 2018 roku*, https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/przedsiebiorstwa-niefinansowe/dzialalnosc-przedsiebiorstw-niefinansowych-w--2018-roku,2,15.html, data dostępu: 12.04.2021r.
[14] Jamka B. (2011), *Czynnik ludzki we współczesnym przedsiębiorstwie: Zasób czy kapitał?* Wolters Kluwer, Warszawa.
[15] Kałużna E., Fellner A. (2014), *Metody uwzględnienia czynnika ludzkiego w zarządzaniu bezpieczeństwem systemu transportu lotniczego*, „Prace Naukowe Politechniki Warszawskiej. Transport", Nr 103, s. 99-111.
[16] 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.
[17] Kobis P., Kisiołek A. (2018), *Zarządzanie bezpieczeństwem danych w przedsiębiorstwach MSP z uwzględnieniem czynnika ludzkiego – wyniki badań*, „Przegląd Organizacji", Nr 8, s. 44–52.
[18] Koźmiński A.K., Jemielniak D. (2008), *Zarządzanie od podstaw. Podręcznik akademicki*, Wydawnictwa Akademickie i Profesjonalne, Warszawa.
[19] KPMG (2020), Raport: Barometr cyberbezpieczeństwa W kierunku rozwiązań chmurowych, https://assets.kpmg/content/dam/kpmg/pl/pdf/2020/06/pl-raport-kpmg-barometr-cyberbezpieczenstwa-2020-w-kierunku-rozwiazan--chmurowych.pdf, data dostępu: 17.04.2021 r.
[20] Mikuła B. (2003), *Czynnik ludzki w nowoczesnych koncepcjach zarządzania*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie", Nr 626, s. 7–22.
[21] Olejniczuk-Merta A. (2015), *Konsumpcja czynnikiem innowacyjnego rozwoju*, „Marketing i Rynek", Nr 2 (CD), s. 5–13.
[22] Oleksyn T. (2018), *Zarządzanie kompetencjami. Teoria i praktyka*, Wyd. III, Wolters Kluwer, Warszawa.
[23] Słownik Języka Polskiego PWN (2021a), *Lekkomyślność – definicja, synonimy, przykłady użycia*, https://sjp.pwn.pl/szukaj/lekkomy%C5%9Blno%C5%9B%C4%87.html, data dostępu: 07.04.2021 r.
[24] Słownik Języka Polskiego PWN (2021b), *Niedbalstwo – definicja, synonimy, przykłady użycia*, https://sjp.pwn.pl/szukaj/niedbalstwo.html, data dostępu: 07.04.2021 r.
[25] Sobolewska S. (2018), *Ochrona informacji marketingowej w przedsiębiorstwie*, „Roczniki Kolegium Analiz Ekonomicznych Szkoły Głównej Handlowej", Nr 49, Społeczno-ekonomiczne aspekty rozwoju gospodarki cyfrowej: koncepcje zarządzania i bezpieczeństwa, s. 113–124.
[26] Tessian (2021), *The Psychology of Human Error*, https://www.tessian.com/research/the-psychology-of-human-error/, access date: 14.04.2021.
[27] Wang Y. (2008), *On Cognitive Properties of Human Factors and Error Models in Engineering and Socialization*, „International Journal of Cognitive Informatics and Natural Intelligence", No. 2(4), pp. 70–84.

Zagrożenia dla bezpieczeństwa informacji wynikające z czynnika ludzkiego w percepcji osób zarządzających zasobami niematerialnymi

Streszczenie

W artykule podjęto temat postrzegania wybranych czynników mających wpływ na bezpieczeństwo zasobów informacyjnych przez osoby odpowiedzialne za zarządzanie zasobami niematerialnymi w mikro- i małych przedsiębiorstwach. Wyszczególniono pięć najczęściej występujących w literaturze czynników zależnych od pracowników, które mogą stanowić przyczynę utraty lub przejęcia przez osoby trzecie kluczowych dla podmiotów gospodarczych informacji.
W części teoretycznej opisano podstawowe zagadnienia dotyczące pojęcia czynnika ludzkiego, natomiast w części empirycznej przedstawiono badania przeprowadzone przez autorów w mikro- i małych przedsiębiorstwach w województwie śląskim. Celem artykułu jest zaprezentowanie roli czynnika ludzkiego w generowaniu potencjalnych zagrożeń dla bezpieczeństwa zasobów niematerialnych przy obsłudze wybranych rozwiązań aplikacyjnych oraz postrzegania go przez pracowników przedsiębiorstw w konfrontacji z technicznymi systemami bezpieczeństwa.

Słowa kluczowe

informacja, przedsiębiorstwo, bezpieczeństwo informacji, czynnik ludzki, kompetencje