Scientific Journal of the Military University of Land Forces
(ISSN: 2544-7122)
2018, Volume 50, Number 1(187), Pages 105-118
DOI: 10.5604/01.3001.0011.7364

Original article

Threats associated with the human factor in the aspect of information security

Michal Palega[1*], Marcin Knapinski[2]

[1]Faculty of Production Engineering and Materials Technology, Czestochowa University of Technology, Poland, mpalega@wip.pcz.pl

[2]Faculty of Production Engineering and Materials Technology, Czestochowa University of Technology, Poland, knap@wip.pcz.pl

INFORMATIONS

Article history:

Submited: 08 May 2017

Accepted: 11 August 2017

Published: 15 March 2018

* Corresponding author

ABSTRACT

The current publication presents selected risks resulting from the involvement of the human factor. In the opinion of the authors of the paper, it is the human inclination to make mistakes, commit breaches and abuses that can generate losses and damages caused by disclosure, modification, destruction or loss of corporate data. Theoretical considerations on the subject matter have been enriched by the results of conducted empirical research. They answer the following question: What categories of information security threats are associated with the human factor.

KEYWORDS

information security, information security management system, information protection, information security threats

1. Introduction

Today, one of the important assets of every business organization is information and in many cases it constitutes a strategic asset. They play the role of an elementary economic factor, determining profit and level of competitiveness on the market [2, 3, 4, 7, 11, 14]. Therefore, there is a need for effective management of information resources. As its basis, it should cover not only shaping of multi-way information flow networks and channels, considering the tendencies and the directions of information management systems development, but also broadly understood issues of information security.

Information security should be perceived as the entirety of technical means and organizational solutions, creating a barrier against threats. These may include: data destruction, its loss, unauthorized copying, modification or disclosure.

Furthermore, it should be very clearly and precisely emphasized that all actions focused on the issue of ensuring a reasonable level of information security should not be treated by a business entity selectively, as a one-time or occasional measure, but as

a continuous process. It should constitute a complex set of solutions, subject to systematic monitoring and development.

The critical factor in the structure of this process remains to be the fully underestimated role of the human factor. Meanwhile, it is precisely the human inclination to make mistakes, commit breaches and abuses that generate losses and damages caused by disclosure, modification, destruction or loss of corporate data.

The purpose of this publication is to draw the reader's attention to the role of the human factor in the information security system of an enterprise. In the opinion of the authors of this work, when organizing proper protection of information resources risks arising from intentional or unintentional activity of an individual must be taken into account. The considerations presented in the article result from the authors' own research conducted in one of the companies operating on the construction services market, located in the Silesian Voivodeship.

2. Information security threats – literature study

A threat should be understood as a potential cause of an event that could result in a breach of security of the information processing system, which creates damage to an organization or its resources. Direct or indirect attack on information may result in damage, disclosure, modification and loss of information or its accessibility.

Information processes in modern business entities are exposed to a number of different threat categories with varying degrees of occurrence probability. As a result, every business activity is burdened with the possibility of a threat. In addition, due to the development of information and communication technology, and especially the Internet, information security threats are becoming more frequent, taking on new and unknown forms and generating enormous losses and damages to an individual, organization, society or even country. The popularity of information systems and computer networks means that they are not free from threats and, additionally, they have created new types of dangers [15, 17]. Consequently, ensuring the adequate level of security requires appropriate identification and classification of threats, as only such activities permit the proper establishment of safety rules and the choice of security measures.

By classifying information security threats based on a criterion such as the source of their emergence, internal and external threats can be distinguished [1, 9, 12, 18]. Internal threats come from legal users of the information system (e.g. company employees) and therefore they are the most dangerous. They may be linked to computer hardware, software or people (organization employees). External threats, in turn, come from the business environment and are usually related to the specific activity of a business entity and the use of the Internet [5]. Most often, they result from intentional or accidental action of third parties, such as intruders attempting to access corporate information.

Considering the technical criterion, hardware and software threats can be distinguished. Hardware threats are caused by malfunction or failure of IT equipment or intentional in-

terference with the system and/or IT network. Software threats are created by software gaps and errors, its failure or unauthorized interference with this software [13].

Information security threats can also be classified with respect to the whole information process, which consists of: collection, processing, storage and transmission of information. At each of these stages, specific threats are generated [10]:

- collection, processing – modification of information;
- storage – unauthorized access, destruction, modification of information;
- transmission – interception, eavesdropping, modification of information.

It is also worth emphasizing that the environment and cultural conditions within which an organization operates can significantly affect the harmfulness of threats and regulate the course of business conduct. In exceptional cases, specific cultural conditions require the recognition of some kind of dangers as harmless.

As indicated above, the identification and assessment of threats should take into account the internal and external sources of their occurrence, as well as the threats resulting from random events. T. Kifner does not share this view and considers the cited classification criteria as merely academic and not reflected in economic practice [6]. In his opinion, the most accurate division includes risks that have consequences related to financial and non-financial losses. Table 1 presents the taxonomy of information security threats, taking into account criteria such as: the role of man, impact object and impact effect.

Table 1. Classification of information security threats

criterion	threats division	examples of threats
Role of man	threats independent from man	lightning, flood, fire, moisture
	threats dependent on man	unauthorized modification of software or data, illegal copying and installation of computer programs, damage or deletion of software or data, theft of computer hardware or equipment, storing collections prohibited by law, errors due to lack of knowledge, distraction, fatigue or neglect of duties resulting in unintentional loss, destruction, deletion or disclosure of information to other unauthorized persons
Impact object	threats related to computer hardware	interruptions in the electricity supply, intentional and unintentional human activities (theft, mechanical damage, configuration errors, improper use or maintenance), failure of computer hardware subassemblies
	threats related to	errors committed by software producers, errors caused by intentional or unintentional human activity

criterion	threats division	examples of threats
Action effect	software	(e.g. improper installation, configuration, administration, scanning, introduction of malicious programs, preventing the proper functioning of applications, unauthorized use, software copying)
	threats related to data	unauthorized browsing, modification, data copying, monitoring (eavesdropping) data, entering false data
	threats related to ICT networks	intentional or unintentional human actions (theft of network component, network physical damage, improper configuration, network blockage, unauthorized network usage, etc.), failures of ICT networks due to physical factors, etc.
	threats related to the human factor	failure to keep enterprise's secrets (conscious and unconscious sharing and transmitting data), sharing information with colleagues or third parties about security systems used in an enterprise, sudden loss or dismissal from work, an employee's transition to the competition
	threats causing financial losses	loss of customers, loss of technology, interruptions in business functioning, loss or destruction of resources, financial penalties, increase in insurance premiums, need to hire additional staff, legal costs, collapse or termination of business activity
	threats creating financial losses	loss of positive image of the company, decrease in credibility of the organization, loss of productivity, endangering the health and life of the personnel, decision errors caused by falsified or incomplete data

Source: own elaboration based on [8]

In the literature of the subject, there is also a division of threats taking into account only the activity of the human factor. It introduces two principal concepts: a source of threat (a threatening unit) and motivation. Individuals who intentionally or unintentionally can use the vulnerabilities to cause losses and damages to organization's resources constitute the source of threat. Motivation means the potential benefits for the threatening individual as well as tools that he or she will use to attack information. Examples of threats involving human participation are shown in Table 2.

Table 2. Threats involving human participation

source of threats	motivation	threats
Hacker, cracker	– personal	– social engineering – unauthorized access to the

source of threats	motivation	threats
	– belief – rebellion	system – systemic intrusion
Computer criminal	– vandalism – financial advantage	– fraud – information bribery – falsifying in the form of spoofing – systemic intrusion
Terrorist	– blackmail – use – vandalism – revenge	– bombs/terrorism – information wars – attack on the system (e.g. distributed denial of service) – system penetration – system manipulation
Business espionage (companies, foreign offices, other government agencies)	– competitive advantages – economic espionage	– economic use – information theft – personal privacy violation – social engineering – system penetration – unauthorized access to the system
Employee (poorly educated, disappointed, dishonest)	– curiosity – ego – intelligence – financial advantage – revenge – accidental error	– intrusion, computer abuse – unauthorized access to the system – assault on employee – blackmail – viewing classified information – frauds and thefts – bribery – introduction of falsified or damaged data – information capturing – malicious code (e.g. viruses,

source of threats	motivation	threats
		Trojan horses, logical bombs) – sale of personal data – system errors – system intrusions – system sabotage

Source: own elaboration based on [16]

3. Preparing and conducting of own research

Opinions and judgments have played a major role in collecting research material, which was possible to achieve by using two research methods: surveying and interviewing.

During the survey, the technique of individual, environmental and anonymous questionnaire was used. In turn, the author's questionnaire was used as a research tool.

The interview was conducted using the technique of uncategorized (free) interview. Its purpose was to supplement and detail questions in the survey questionnaire. Taking into account the applied research technique, the research material was collected using a tool in the form of an interview questionnaire.

Selected research results are cited further in this publication. They served to answer the following question: What categories of information security threats are associated with the human factor? The research conducted is a valuable source of information, enriching the knowledge of the issues discussed in this publication, and its results are a perfect complement to the theoretical considerations.

4. Taxonomy of information security threats associated with the human factor

Regardless of the variety of information security threats, the human factor should be recognized as the main source of their origin. The conducted research has shown a number of threats that have been categorized into four groups. The first of them consists of intentional actions of employees, dictated by their low motivation, bad working atmosphere, lack of sense of association with a company and shared responsibility for its security as well as the desire to make a quick profit.

The research results showed that 45% of respondents pointed to theft of equipment, documents or mobile data carriers as the most important sources of information security threats in an enterprise. With regard to intentional threats, violating existing security rules and procedures by employees were also taken into account. The findings related to personnel behaviors determining the loss or disclosure of corporate data are summarized in Figure 1.

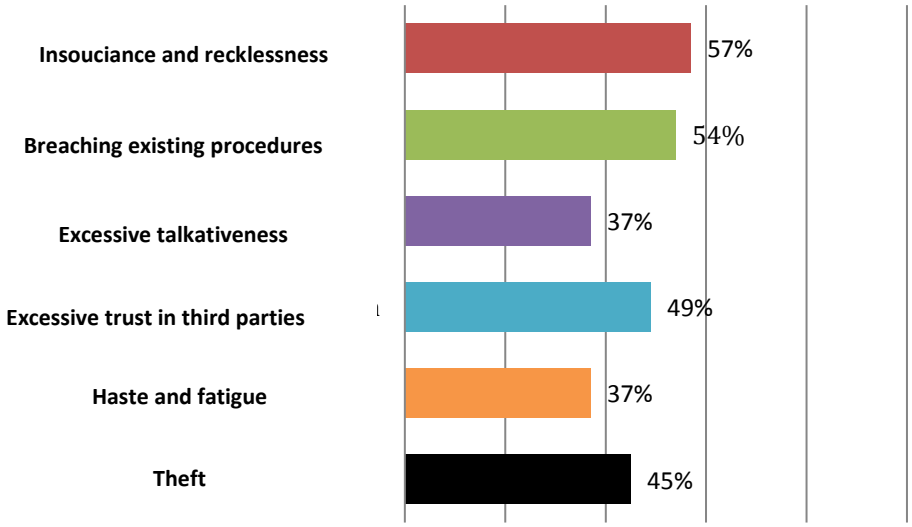

Fig. 1. Personnel behavior that may lead to the loss/disclosure of information

Source: own elaboration based on the conducted research

Furthermore, the conducted research results indicate that employees violate procedures regarding the usage of computer hardware and company e-mail box. More than half (63%) of the respondents used company e-mail also for private purposes and as much as 80% used company computer hardware to browse websites not related to official duties, as the data in Figure 2 shows.

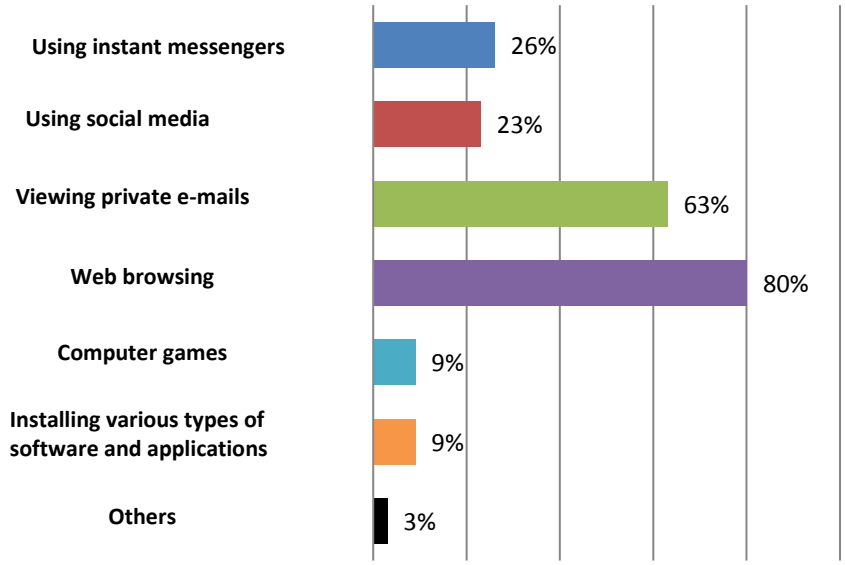

Fig. 2. The usage of business computer hardware for private purposes

Source: Own study based on the conducted research

The second group of human factor threats results from the executives' insufficient knowledge in the scope of information security management, which in turn translates

into lack of adequate skills of perceiving and counteracting threats among other employees.

Only persons with access to legally protected information (personal data) participate in training courses, as such an obligation is imposed by adequate legal regulations. The rest of employees, including mainly temporary ones, interns and trainees, do not take part in any form of further training. It can be seen from the data in Figure 3 that only 26% of the respondents indicated that the company had organized information security courses and trainings, while 45% of them claimed that they had participated in such forms of additional education, as shown in Figure 3.

The third group of threats is related to using various ways of manipulating people, influencing their emotions or tricking them. This is inextricably linked to the above-mentioned group of threats, since social engineering attacks are usually aimed at people with low awareness in the field of threats and the company, which lack the adequate training among both employers and employees in an enterprise.

Social engineering primarily uses human weaknesses such as: human tendency to help, excessive talkativeness, excessive trust, vulnerability to the impact of third parties, etc. The conducted survey research has confirmed that they are one of the most important factors determining the loss of information security of an enterprise (Figure 1).

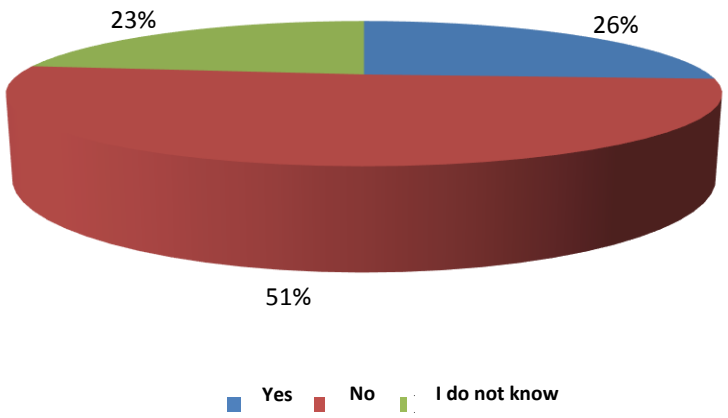

Fig. 3. Organization of information security courses and trainings

Source: own elaboration based on the conducted research

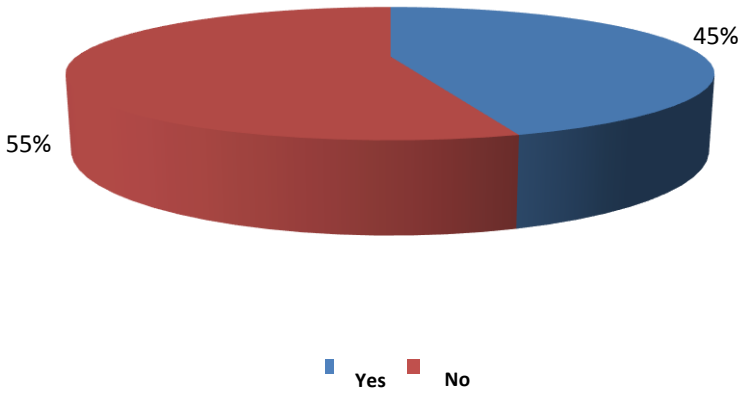

Fig. 4. The participation of employees in information security courses and trainings

Source: own elaboration based on the conducted research

The fourth group results from inadequate organization of work. Among many irregularities, the following can be identified:

Short-staffing in the sphere of information security management. During the survey, the highest percentage of respondents indicated the company's chief IT specialist as a person responsible for information security in the company, while only 10% of respondents pointed to the information security specialist, as evidenced by Figure 5.

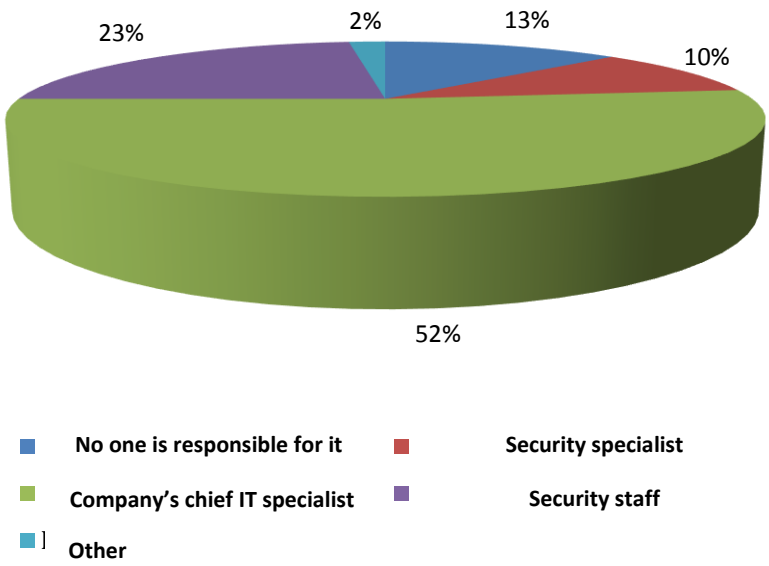

Fig. 5. The structure of enterprise personnel responsible for information security

Source: own elaboration based on the conducted research

Accordingly, the widespread belief that information security is, above all, the elimination of threats in the IT infrastructure has been confirmed. The lack of information security specialists in the organizational structure can contribute, among other things, to:

improper classification of information, gaps and errors in the intra-corporate information flow system and its distribution outside, personnel's incompetence and unawareness in terms of vulnerability to threats or ineffectiveness of implemented security measures (especially the organizational ones).

Improper staff motivation. Low employee motivation fosters intentional actions against a company, which surely includes information theft. This aspect was touched upon while discussing the first group of threats.

Deficiencies in the personnel assessment and development system. In situations where an employee feels unappreciated, disrespected and does not feel attached to the company as well as the shared responsibility for its financial performance or security, he or she will commit a crime related to, for example, information theft faster and easier.

Deficiencies and errors in the system of training and raising awareness among employees. Ignorance and unawareness of employees are one of the primary sources of loss or disclosure of corporate information. Therefore, every organization should strive for the highest possible level of its employees' knowledge. The conducted research showed that the reality is different. It can be concluded from the empirical data that only half of the employees participated in courses or trainings. The effectiveness and usefulness of the workshops is also a serious problem. The research proved that nearly half of respondents were unable to identify practical applications resulting from the content of the completed training. Based on the empirical data, it can be said that only 6% of respondents saw the usefulness of teaching material for the existing conditions in an enterprise to a large extent. A summary of the research results in the field of the usefulness assessment of completed trainings and courses for the daily tasks is depicted in Figure 6.

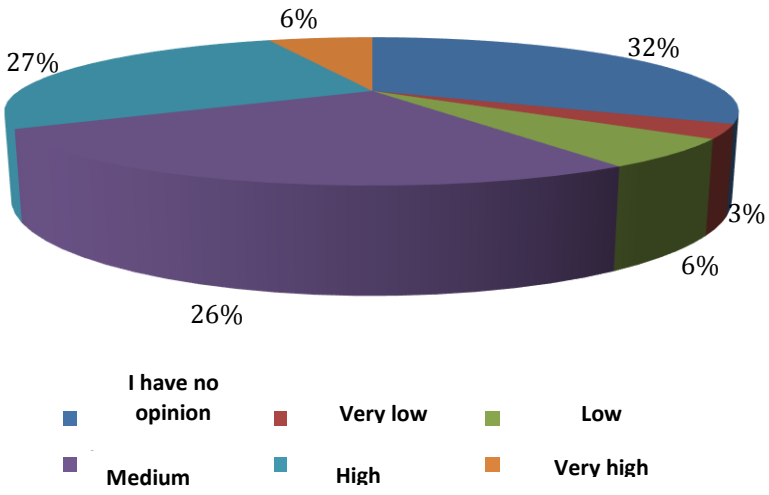

Fig. 6. The usefulness of information security courses and trainings for daily work

Source: own elaboration based on the conducted research

Staffing inadequate for delegated duties. Workplace underemployment can cause employees haste and fatigue as well as excessive stress, which obviously affect the quality

of performed work and contributes to mistakes committed by employees, such as sending messages containing confidential data to a wrong email address, losing or accidental destruction of mobile data carriers. The data in Figure 1 evidence that 37% of respondents believed that employee haste and fatigue were one of the most important factors fostering the loss or disclosure of corporate data.

Conclusions

Information is one of the elementary resources of an enterprise, essential in the decision-making process and organization management. In modern business space, it is treated as a special immaterial good, which, alongside other resources, has a specified value that determines success in business activity. Thus, organizations are obliged to ensure a reliable level of confidentiality, integrity and accessibility of processed and stored information and data. All events and incidents related to a breach of information security may adversely affect the functioning of an enterprise, undermine its competitive position and result in serious financial losses.

The holistic approach to information security management assumes that it is a continuous process, based on technical and procedural solutions as well as human action. Currently, it is generally accepted that the human factor is the weakest link in the information security chain. Human nature and social interactions can be much more easily manipulated than technologies and information systems designed for the protection of information.

The conducted survey research show that the biggest threat is connected with intentional actions of employees, which may include, among others, theft, economic espionage or non-compliance with the main security principles of a company. Such behaviors may be determined by dissatisfaction with earnings, refusal to increase them, refusal of promotion or discontent with working conditions. Consequently, information security management should include the development of guidelines for disciplining and motivating staff.

The empirical research also male it possible to assert that an important group of information security threats comprises of those resulting from insufficient knowledge and involvement of executives in information security management issues, which is reflected in the attitudes and behavior of other employees in the company. The lack of systematic training of employees undoubtedly constitutes a serious problem in the examined entity. The survey research indicates that only 26% of respondents declared that their company organized courses and trainings related to information security, while 45% of respondents participated in such trainings. Furthermore, in the light of the research conducted, difficulties resulting from pointing out the usefulness of training content for implementation of daily duties were determined. Only 27% of respondents rated the usefulness of training as high and 6% - as very high. Hence, gaps and errors in employee training constitute another threat caused by the human factor. Therefore, drawing attention to shaping awareness of threat occurrence as well as responsibility for protecting processed data and information is the necessary action in the scope of information security management.

Based on the above, it is necessary to take action aimed at managing the human factor, which in general should consist of:

- precise determination of employees' duties and powers;
- providing all necessary resources to employees (work tools);
- establishing appropriate rules for hiring employees and monitoring their work (reliability, honesty, work ethics, reputation and competence);
- handing over materials to employees regarding the valid procedures and security systems used;
- continuous training and raising awareness among personnel;
- using clear human resources politics and rules on introduction and withdrawal of employment procedures.

Acknowledgement

No acknowledgement and potential founding was reported by the authors.

Conflict of interests

The author declared no conflict of interests.

Author contributions

All authors contributed to the interpretation of results and writing of the paper. All authors read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.

ORCID

The authors declared that they have no ORCID ID's

References

1. Benson S., Standing C., *Information Systems. A Business Approach,* John Wiley & Sons, 2002.
2. Borowiecki R., Czekaj J., *Zasoby informacyjne w ograniczaniu ryzyka gospodarczego,* Dom Organizatora, Torun 2011.
3. Flakiewicz W., *Systemy informacyjne w zarządzaniu,* PWN, Warszawa 1990.
4. Grabara J.K., Kisielnicki J., Nowak J.S., *Informatyka i wspólczesne zarządzanie,* PTI, Katowice 2005.
5. Hamrol A., *Zarządzanie jakością z przykladami,* PWN, Warszawa 2005.

6. Kifner T., *Polityka bezpieczenstwa informacji,* Helion, Gliwice 1999.
7. Klos Z., Klos J., *Wybrane pozanormatywne aspekty zarządzania bezpieczenstwem informacji,* Problemy jakości 2007.
8. *Komputerowe wspomaganie biznesu,* (ed) A. Nowickiego, Placet, Warszawa 2006.
9. Kusina B., *Analiza ryzyka raz jeszcze…,* Ochrona Mienia 2000, nr 9.
10. Luczak J., Tyburski M., *Systemowe zarządzanie bezpieczenstwem informacji ISO/IEC 27001,* UE, Poznan 2010.
11. Olesinski J., *Ekonomika informacji. Metody,* PWE, Warszawa 2003.
12. Pipkin D.L., *Bezpieczenstwo informacji. Ochrona globalnego przedsiebiorstwa,* WNT, Warszawa 2002.
13. *Procesy informacyjne w zarządzaniu,* (ed) A. Nowicki, M. Sitarski, UE, Wroclaw 2010.
14. Stefanowicz B., *Informacja*, SGH, Warszawa 2005.
15. *Technologie informacyjne dla ekonomistów. Narzedzia, zastosowania*, (ed) Nowicki A., WUE, Wroclaw 2008.
16. Wolowski F., Zawila Niedźwicki J., *Bezpieczenstwo systemów informacyjnych,* edu – Libri, 2012.
17. *Wstep do systemów informacyjnych zarządzania w przedsiebiorstwie,* (ed) A. Nowicki, PCz, Czestochowa 2002.
18. Żebrowski A., Kwiecinski M., *Bezpieczenstwo informacji III Rzeczypospolitej,* Abrys, Kraków 2000.

Biographical notes

Michal Palega – Dr. Eng. in Production Engineering; he received a scientific title in 2016 at the Czestochowa University of Technology at the Faculty of Production Engineering and Materials Technology. The topic of his doctoral thesis concerned the role of the human factor in the enterprise information security system. He is employed as an assistant professor at the Institute of Metal Forming and Safety Engineering at the Faculty of Production Engineering and Materials Technology at the Czestochowa University of Technology. Participant of information security conferences and training, including personal data and classified information. Internal auditor of the information security management system according to ISO 27001: 2013. Main areas of interest are: safety engineering, information security management and crisis management.

Marcin Knapinski – Dr hab. Eng. Currently employed as an associate professor at the Institute of Metal Forming and Safety Engineering at the Faculty of Production Engineering and Materials Technology at the Czestochowa University of Technology, where in the term 2012-2016 he was Deputy Dean for Science, and in the term 2016-2020 he has held the office of Dean. Secretary of the Production Engineering Committee of the Polish Academy of Science and a member of the Sections of the Metallurgy Committee

of of the Polish Academy of Science. His scientific-research activities focus on the following areas: numerical and physical simulations of metal forming processes, design and optimization of plastic processing, mechanical properties of metallic materials, automation of industrial processes, safety engineering and information security management. He is the author and co-author of 1 monograph, 2 scientific dissertations and over 260 publications in journals, chapters of monographs and conference materials.

How to cite this paper

Palega M., Knapinski M., (2017) – Threats associated with the human factor in the aspect of information security. *Scientific Journal of the Military University Of Land Forces*, vol. 50, no. 1 (182), p. 105-118, http://dx.doi.org/10.5604/01.3001.0011.7364