sciendo CzOTO 2019, volume 1, issue 1, pp. 132-140

ASSESSMENT OF EMPLOYEES LEVEL OF AWARENESS IN THE ASPECT OF INFORMATION SECURITY

doi: 10.2478/czoto-2019-0017
Date of submission of the article to the Editor: 29/11/2018
Date of acceptance of the article by the Editor: 25/01/2019

Michał Pałęga[1] – *orcid id: 0000-0002-2779-431X*
Marcin Knapiński[2] – *orcid id: 0000-0001-8817-2250*
[1]Czestochowa University of Technology, **Poland,** *palega.michal@wip.pcz.pl*
[2]Czestochowa University of Technology, **Poland**

Abstract: The strategic importance of information for the functioning of each economic entity forces entrepreneurs to properly protect them against loss, unauthorized disclosure or unauthorized modification. Hence, organizations build complex security systems taking into account state-of-the-art technical solutions, while belittling often the most important element, which is the human factor. It should be emphasized that it is the intentional or accidental actions of the human that can lead to the loss of information security. In addition, it is also the potential of human capabilities and skills can provide an effective defense against the failure or technical security.
The article presents the basic stages of human resource management in the aspect of information security. Complementing these considerations will be the presentation and discussion of the results of surveys aimed at assessing the level of employee awareness in the area of information security.
Keywords: Information security, data protection, information security management, human resources management

1. INTRODUCTION

Information is one of the basic resources of modern enterprises and organizations. They decide on gaining a competitive advantage, maintaining the level of innovation, as well as achieving success on the market. Therefore, all economic entities striving to achieve the set strategic goals and shape a credible image on the market are obliged to ensure the security of processed and stored information (Antoniou, 2018; Kifner, 1999; Wołowski, Zawiła-Niedźwiecki, 2012).
Information security should be understood as the preservation of its three basic attributes, which include: confidentiality, integrity. In addition, other properties such as authenticity, accountability, non-repudiation or reliability can be taken into account (PN-EN ISO/IEC 27000:2017-06). This confidentiality will ensure that only authorized persons or entities have access to a specific set of information, data or system. Data integrity means that data has not been altered, modified or distorted

without the knowledge of their owners. However, the availability of data means that the system and data can be used continuously by authorized users. Today, threats related to the loss of information security are treated as one of the most important areas of operational risk. Therefore, they require proper conduct, reducing the possibility of their occurrence and the level of possible consequences (.Burdak, Sobczak, 2014; Herath T. Herath H., D'Arcy, 2017; Janczak, Nowak 2014). Taking the above into consideration, the information security policy should be part of the strategy of each company. It should also be emphasized that the development of procedures and instructions for conduct is insufficient, but the employees' awareness of the responsibility for information security is essential.

A frequently encountered statement, both in the literature of the subject and also among specialists dealing with data protection, the weakest element of information security is the human factor. It is the human inclination to make mistakes and adulteration and abuse that may result in the loss or disclosure of company information (Amankwa, Loock, Kritzinger, 2018; Pałęga, 2015; Palega, Knapinski, 2017). Nevertheless, in the belief of the authors of this publication, it is also the potential of human skills, capabilities, ideas, commitment and motivation of employees can be an effective defense against the failure of technical security.

The article presents an analysis of the results of surveys concerning the assessment of employees' awareness in the field of information security. The considerations presented in the work concern, among others:

- the necessity for employees to comply with the rules on information security,
- perceiving the disclosure / loss of information as a real threat,
- awareness of employees that their careless and reckless actions may be the reason for the loss or disclosure of information,
- identification of human behavior conducive to the loss of information security,
- handling of personnel with sensitive company information.

The results carried out graphically are presented on a pie chart. The distribution of responses is shown in percent.

2. SUBJECT OF RESEARCH

The research was carried out in a selected industrial enterprise in the construction services sector. The analyzed company offers its clients such services as: execution of construction works, steel structures and technological devices. However, its basic domain is the construction of sewage treatment plants and sewage systems, carried out on behalf of local governments. In addition, the company uses its own design facilities and a research laboratory. For this reason, the issue of information security becomes particularly important.

3. RESULTS – ASSESSMENT OF THE AWARENESS OF THE COMPANY'S PERSONNEL IN THE AREA OF INFORMATION SECURITY THREATS

Ensuring effective protection against security risks requires the use of technical safeguards in combination with security procedures, which are the benchmarks for the behavior and conduct of employees along with the appropriate theoretical and practical training.

Having trained, aware, vigilant and complying employees in compliance with the applicable rules allows employees to limit the threats resulting from the activity of the human factor, and mainly social engineering attacks.
The results of own research regarding the level of staff awareness in the area of information security threats are presented below.
The need to comply with rules and procedures is one of the main factors of information security. The basic responsibility of each company is to develop in writing rules, procedures and recommendations relating to the security of information resources. However, it should be borne in mind that these studies can not only be the so-called "Dead records". It is the responsibility of the organization's management to oblige all employees who have access to information or IT systems to respect them (Pałęga, 2015)
The results of the research allow to conclude that the surveyed organization implements effective programs of building staff awareness – 89% of all respondents declare that they perceive the need to proceed in accordance with the standards and standards in the field of information security (Fig. 1).

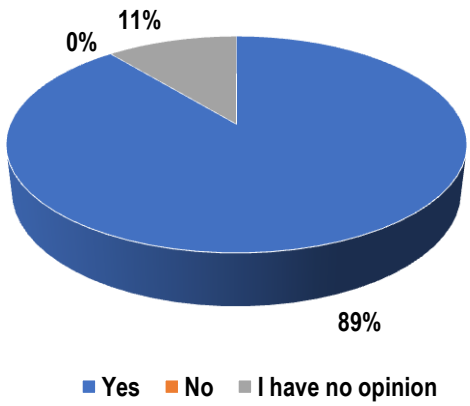

Fig. 1. Awareness of the need to follow rules and procedures information security
Source: own elaboration based on the conducted research

The perception of loss or uncontrolled disclosure by the staff as a real threat is another important factor in information security. The organization's staff must know that the loss, destruction or uncontrolled modification of information and related damage can actually happen. Only this approach to losing the attributes of information security will positively affect all human activities. Therefore, all training programs should be based on presenting specific cases of attacks on information and analysis of losses suffered by their victims. Both entire enterprises, as well as individuals who are taught by the bad experience of other institutions, will pay more attention to information security practices and procedures (Pałęga, 2015). Data regarding this area of research are presented in Fig.2.

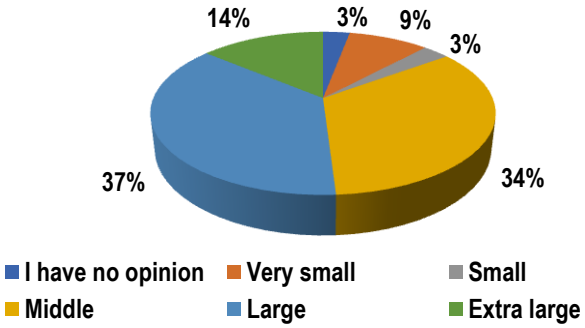

Fig. 2. Perceiving the disclosure / loss of information as a real threat
Source: own elaboration based on the conducted research

The analysis of empirical data allows to state that modern organizations are aware of the fact that the loss / disclosure of information and various types of incidents that disrupt the security of information assets are a real threat. Research shows that this view is shared by 85% of respondents (14% considered the threat as extra-large, 37% - large and 34% - medium).
Survey research also concerned the role of the employee in the occurrence of information security incidents. As noted earlier, the most important issue of information security systems is the human factor that can destroy the most technologically advanced security features. Regardless of the level of knowledge and skills, people will always be the greatest threat. Security is therefore not a technological problem. It is connected above all with the right approach to the management of the organization and its resources. It should be remembered that breaking the human barrier is much easier and less capital intensive than penetrating the company's IT system. Therefore, all employees of the company should be aware that their inattention, willingness to help, insufficient knowledge or the tendency to error can be used by people from within or outside the organization. As a result, they may contribute to the loss of confidentiality of information, exposing the organizational unit to damages and losses (Pałęga, 2015). The results of the research concerning the extent to which the employee himself can be a source of information security loss are presented in Fig. 3.

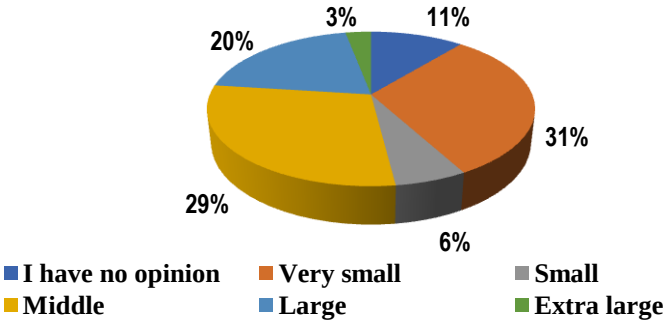

Fig. 3. The degree to which the respondent can contribute to the disclosure / loss of information
Source: own elaboration based on the conducted research

The conducted research shows that only 3% of respondents think that to a very large extent loss or disclosure of confidential data from the company may be due to their fault. However, the results of the survey show that a much larger percentage

of employees are acting irresponsibly, what may contribute to the loss of proprietary information (Pałęga, 2015). Fig. 4 presents the results of research on selected behaviors of employees, which may cause the loss of information security.

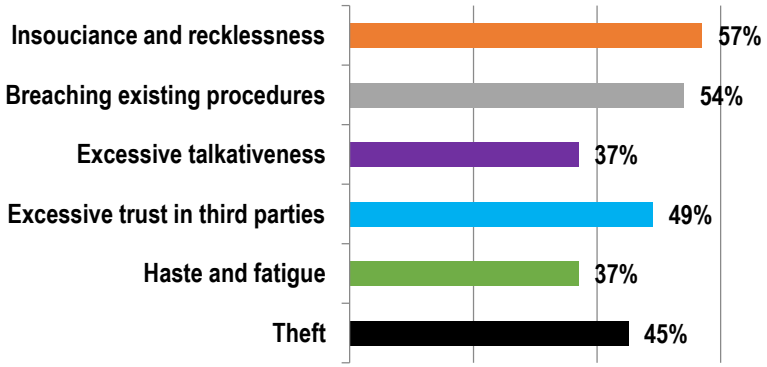

Fig. 4. Personnel behavior that may lead to the loss/disclosure of information
Source: own elaboration based on the conducted research

Among the most undesirable phenomena associated with improper conduct of employees dominates: lightheartedness and recklessness (57%), violation of applicable procedures (54%), or excessive trust in third parties (49%). In turn, for nearly half of the respondents, one of the most important factors determining the loss or disclosure of information is their theft (45%). The conducted research also indicates that excessive talkiness (37%) and haste and fatigue (37%) are perceived by respondents as the least frequent occurrences in organizational units of incidents related to the loss of confidentiality, integrity and accessibility of information. In addition, the conducted research shows that an example of negative behavior of employees in the aspect of information security may be: improper utilization of documents, generation of passwords with low resistance to breaking, use of company hardware and e-mail for private purposes, communication with contractors via social networks (Pałęga, 2015).
The research results indicate that 77% of employees do the right thing in the case of document utilization, using a shredder. In turn, nearly ¼ of respondents declare that they do not use this type of equipment, exposing corporate data to their repeated reproduction and use (Fig. 5).

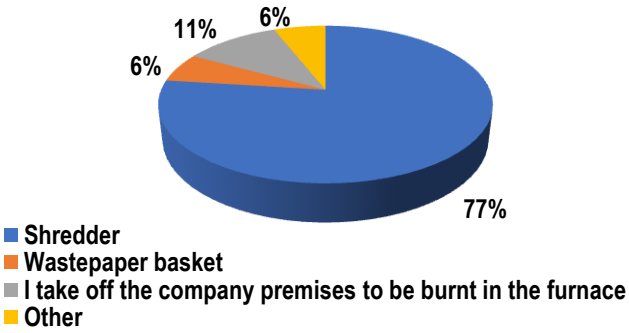

Fig. 5. Ways of getting rid of useless documents containing sensitive information
Source: own elaboration based on the conducted research

In view of the above, it is recommended that the management of the company should ensure that each office station is equipped with a shredder, and additionally materials that warn against the improper utilization of useless documents (leaflets, brochures, etc.) (Pałęga, 2015).
Another aspect of the study was the security of login and access passwords created by employees for computer hardware and applications. The results are presented in Fig. 6.

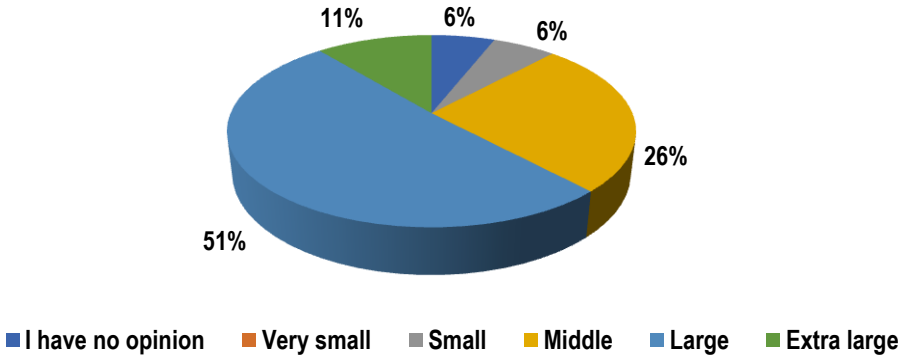

Fig. 6. The security level of the passwords and logins used by employees
Source: own elaboration based on the conducted research

Out of all respondents, 51% admit that their logins and passwords are characterized by a high level of security and 26% by medium. Very strong passwords are generated by only 11% of users. Surveys indicate that employees are not fully aware of the importance of securing the computer system with unauthorized access to it. Therefore, it is recommended that employees be protected against the generation of easily broken passwords. It is also worth considering introducing significant modifications to the password policy, e.g. one-time passwords, software that prevents the creation of too weak passwords, etc.
The indicated research results show how important for the information security system are the daily routine behavior of employees. Effective counteracting this type of undesirable behavior should include shaping the proper organizational culture among the entire staff.

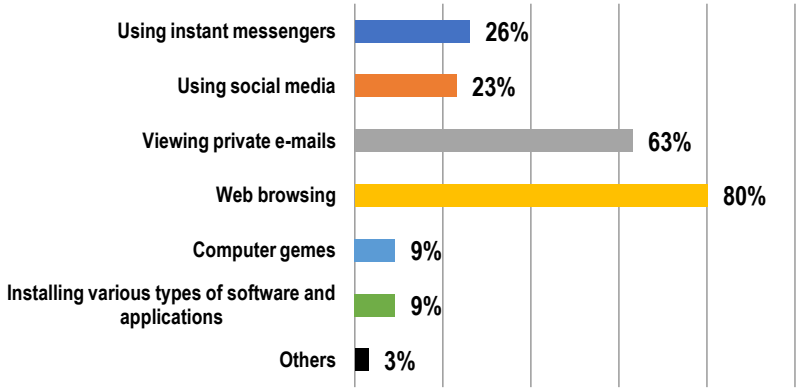

Fig. 7. The usage of business computer hardware for private purposes
Source: own elaboration based on the conducted research

The proper use of work equipment entrusted to the employee is also important to ensure an appropriate level of information security. Research shows that 80% of the total use of computer equipment by employees for private purposes concerns visiting websites. In addition, 63% of employees admit that they use private e-mails, while 26% use instant messaging. On the other hand, 23% of all respondents register and log on to social networks (Fig. 7) (Pałęga, 2015).
The research results presented above show the scale of the phenomenon of using business computer equipment for private purposes. Certainly they are not optimistic, because its effects can be huge. Examples include hacking into computer systems or taking over passwords and credentials.
Summing up the previous considerations, it should be noted that one of the most important issues related to ensuring information security is the human factor that can destroy the most technologically advanced security features. Regardless of the level of knowledge and skills, people will always be the greatest threat. Security is therefore not a technological problem. It is connected above all with the right approach to the management of the organization and its resources. It should be remembered that breaking the human barrier is much easier and less capital intensive than penetrating the company's IT system. Therefore, all employees of the company should be aware that their inattention, willingness to help, insufficient knowledge or the tendency to error can be used by people from within or outside the organization (Pałęga 2015).

4. CONCLUSION

Reading this publication allows to formulate the following conclusions and final statements:

1. In the situation when the competitiveness of the company is decided by: flexibility of operations, fulfillment of customer expectations, speed and rationality of response to changes in the requirements of the environment, current, full and reliable information is of great importance to the organization. Therefore, currently they are included in the group of basic assets of each enterprise. Information, due to its strategic importance, is characterized by a certain value (often material), and also constitutes the main component of the decision-making process and the production factor. The development of communication and IT technologies has also increased the importance of information in business management and made it possible to process them quickly and less frequently and exchange them with the environment.
2. Information perceived as resources constituting one of the foundations of a company's success or failure requires its proper protection against various threats. These threats include their disclosure, uncontrolled modification, destruction or theft. In today's world, dominated by Internet technology, attacks on information are increasingly being made, the purpose of which is to gain them by competitive entities. Therefore, enterprises are obliged to build and improve their own, individualized information security management system.
3. The presented considerations show that an important element of the information security management system is the human factor. Therefore, organizations should include in their security policies such aspects as:

recruitment of employees, their schooling awareness and motivation, as well as the departure and dismissal of employees. In addition, in the opinion of the authors of the publication, effective human factor management should focus not only on the proper organization of work (work regulations, procedures, instructions), but also building a culture of information security (values, norms, rules) and taking individual incentives to individual behavior (experience, emotions, attitudes, motivations of a specific person). Taking into account the above elements in the information security system may result in employees acting in a responsible manner and complying with the rules governing data protection issues.

4. The results of the surveys presented indicate that the employees of the analyzed enterprise are aware of the need to proceed in accordance with the standards and standards set in the field of information security. This is extremely important as attaching importance to the information security policy guidelines can reduce the risk of information security threats.
5. The conducted research shows that among the inappropriate behaviors of employees related to information security dominate such as:

- generating passwords with low fracture resistance;
- improper utilization of documents;
- communication with contractors via social networks;
- use of company's computer equipment and e-mail for private purposes.

REFERENCES

Amankwa E., Loock M., Kritzinger E., 2018. *Establishing information security policy compliance culture in organizations*. Information and Computer Security 26(4), pp. 420-436.

Antoniou G.S., 2018. *A Framework for the Governance of Information Security: Can it be Used in an Organization*. Conference Proceedings - IEEE SOUTHEASTCON 2018-April, 8479032.

Brdulak J.J., Sobczak P., 2014. *Wybrane problemy zarządzania bezpieczeństwem informacji*. SGH, Warszawa.

Herath T.C., Herath H.S.B., D'Arcy J., 2017. *Managing security in organizations: Adoption of information security solutions.* SIGMIS-CPR 2017 - Proceedings of the 2017 ACM SIGMIS Conference on Computers and People Research pp. 87-88.

Janczak J., Nowak A., (2013), *Bezpieczeństwo informacyjne. Wybrane problemy*, AON, Warszawa.

Kifner T., 1999. *Polityka bezpieczeństwa i ochrony informacji*. Helion Gliwice.

Palega M., 2015. *Rola czynnika ludzkiego w systemie bezpieczeństwa informacji w przedsiębiorstwie*. Praca doktorska napisana pod kierunkiem dr hab. inż. Marcina Knapińskiego, prof. PCz, WIPiTM. Częstochowa.

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

PN-EN ISO/IEC 27000:2017-06. Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia. PKN. Warszawa.

Wołowski F., Zawiła-Niedźwiecki J., 2012. *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*. Edu-Libri. Kraków-Warszawa.