sciendo CzOTO 2021, volume 3, issue 1, pp. 64-70

INFORMATION SECURITY IN INFORMATION SYSTEMS AMONG EMPLOYEES OF INDUSTRIAL ENTERPRISES AS SOCIETIES 5.0

doi: 10.2478/czoto-2021-0007
Date of submission of the article to the Editor: 29/12/2020
Date of acceptance of the article by the Editor: 10/03/2021

Żywiołek Justyna[1] – *orcid id: 0000-0003-0407-0826*
Ali Abdulhassan Abbas[2] – *orcid id: 0000-0001-6860-2583*
[1]Częstochowa University of Technology, **Poland**
[2]University of Kerbala, **Iraq**

Abstract: The article presents the results of research on employee awareness of information security. The essence and methodology of society 5.0 was discussed. The study was an introduction to the study and was carried out in two groups of enterprises, the so-called ordinary and tycg constituting employees of the society 5.0. The strength of the relationship between individual security elements and those supporting society was also presented. 5.0.
Keywords: society 5.0, safety information, safety systems.

1. INTRODUCTION

The world is currently facing many changes, not only technological, but also economic, geopolitical and mindset. We must remember that each change creates new opportunities and challenges. Undoubtedly, creativity and imagination should be the key to shaping the future (Żywiołek, 2018). It is equally important to skilfully use the opportunities offered by technology to acquire new knowledge and create new values, creating connections between people and objects, and between real and virtual worlds (Tutton, 2010). It offers new opportunities to search for and find effective ways to solve problems in society, create better living conditions, and maintain proper economic growth. The idea of Society 5.0 is not a utopian vision of the future, but is a concept that shows one version of the future towards which the world is heading, or at least the richer part of it (Thomas, 2018). The article presents the basic assumptions of information security in information systems among employees of industrial enterprises as societies 5.0. The aim of the article is to examine the existing relations between information security and behavior / solutions proving the functioning of the employee as a society 5.0. The study was conducted thanks to a questionnaire among employees of 5 production companies.

2. INFORMATION SAFETY

The information security management process can be defined as a set of activities that include planning, decision making, organizing and leadership targeting the resources of an organization with the intention of achieving goals efficiently and effectively (Lee, 2018). The goal of information security management is to achieve and maintain a defined level of information processing security and to guarantee confidentiality, integrity, availability, accountability, authenticity and reliability of data (Żywiołek 2016). An important element in the information security management process are: resources, threats, vulnerability, consequences, risk, security and partial risk.

The process of information security management in an enterprise can be presented as mutual relations at the level of creating an information security policy (Łuczak, Tyburski, 2010), its implementation and maintaining the achieved level of security in the current activity of the organization. The company's security policy defines the directions and tasks within the company, the consideration of which guarantees the achievement of the assumed goals, strategy, responsibility, security methods needed to define information classes, most often requiring different levels of security and data protection. Information security is not only about policy documentation, it takes place in three areas (Figure 1).

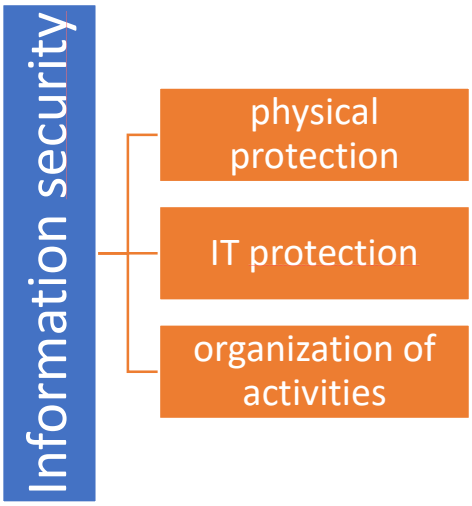


Fig. 1. Information safety

Authors who write about information security often consider only one aspect. IT specialists who notice only systems, technological innovations and often the IT aspect are outsourced and employees have no real influence on problems and security (Horton, 2018). Inspectors and auditors worry about procedures and documentation to undergo another inspection (Stewart, 2009). And physical security is most often used for video monitoring, and unsupervised (Griffy-Brown, Earp, Rosas, 2018). Often, physical protection is associated with the caretaker, which is completely wrong. The authors studying the phenomenon of physical access emphasize the importance of procedures and the use of technological innovations (access cards), and they were the first to alarm about the interpenetration and cooperation of all three areas.

3. SOCIETY 5.0

The Japanese argue that the fifth-numbered society is the next stage of evolution after the model based on hunting (1.0), agriculture (2.0), industry (3.0) and information (4.0).

All of Japan is to aspire to the 5.0 society, and the concepts have been included in the government's technological development plan (Colwill, 2009). Thanks to this socio-technological engineering, the problem identified in the previous version number four is to be overcome. Modern information-based society has difficulties with effective sharing of data and acquired knowledge. The Japanese concept calls this a limitation, without overcoming it, one cannot expect to jump to a higher level of development.
In society 5.0, the world of people, machines and their entire environment is connected and knows how to communicate with each other. The concept assumes something more than the Internet of Things environment announced for years, in which an intelligent processor-processor kettle with a smart refrigerator will exchange information about its owners, in our absence, they will do shopping online together, brew their favorite coffee and order an equally intelligent washing machine to clean the house. Future (Axelrod, Bayuk, Schutzer, 2009). The artificial intelligence from the Japanese plan will work at a higher level of abstraction. Thanks to it, the traffic of autonomous vehicles will be possible on the streets, cities will stop congestion, huge portions of data will be instantly analyzed, smart factories will offer a new quality of the production process, and people will be seriously relieved of their current duties. Society 5.0 is illustrated in Figure 2.

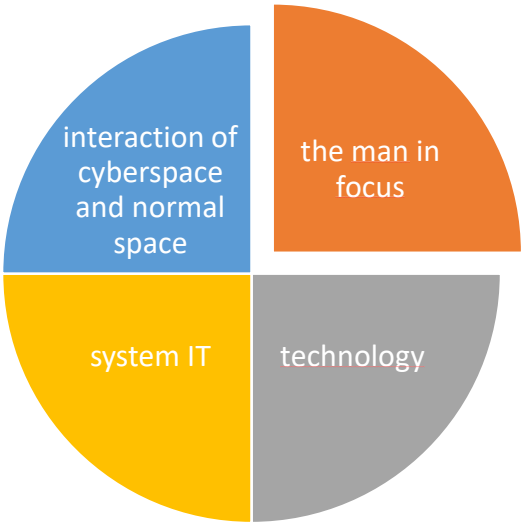


Fig. 2. Society 5.0

Model 5.0 will combine the ability to collect health data on an ongoing basis from patients. Smart gadgets will monitor their parameters, algorithms will analyze the information, and the system will efficiently find resources that will be available.

4. RESEARCH GROUP AND METHODOLOGY

It was a preliminary study, carried out on a group of 5 enterprises, 2 normal and 3 declaring being a society 5.0. The study was conducted based on a questionnaire and personal interview with senior managers. qualitative factors were distinguished and the relations between them and the strength of these relations were established thanks to the C pearson factor (Fig 3.)

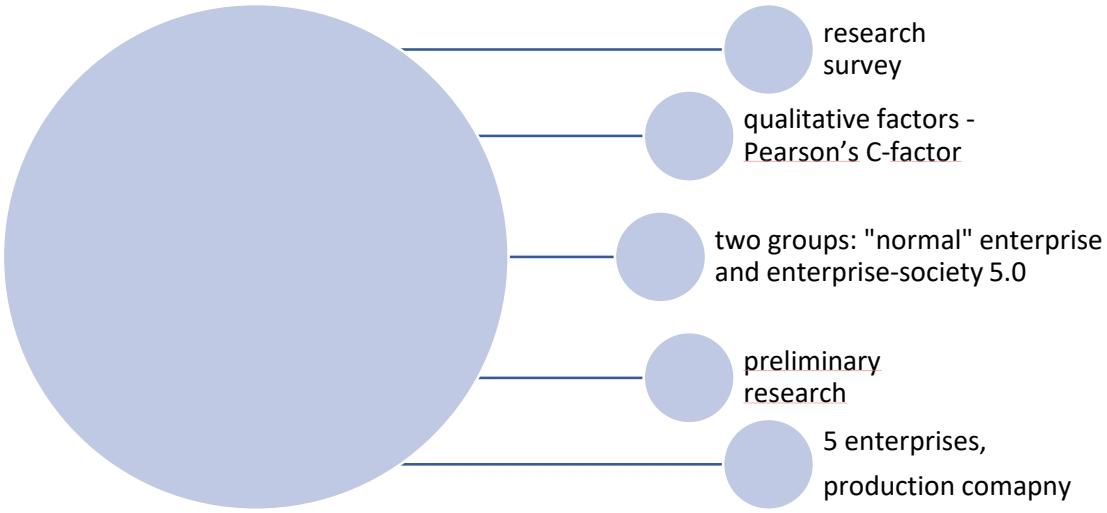


Fig. 3. Research

The survey was conducted among employees of the described research group, using a questionnaire. This is a preliminary study, so the group of the buffalo has not been defined in detail.

5. RESULTS

The respondents assessed selected aspects of security and the perceived elements of being a society 5.0 (Fig. 4).

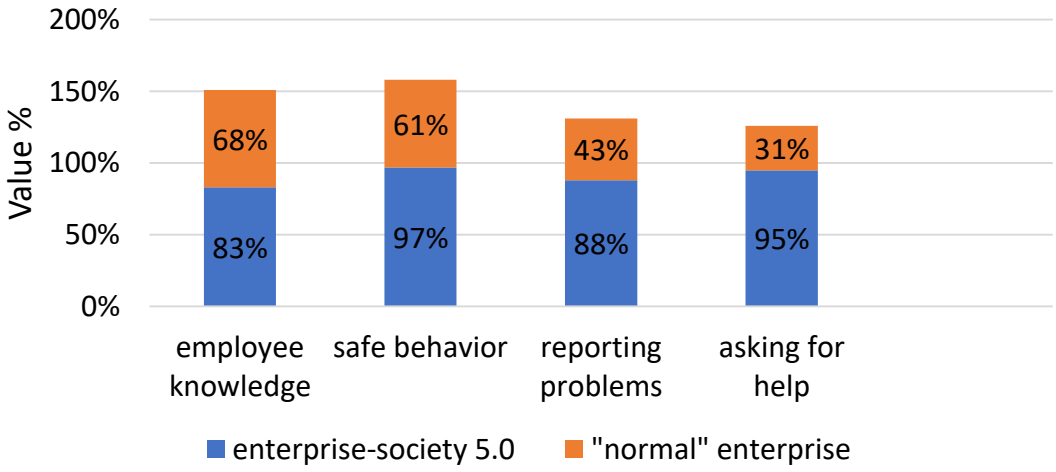


Fig. 4. Elements that society 5.0 and information security in the surveyed enterprises

A significant difference is noticeable in each of the examined aspects, 5.0 enterprises are rated incomparably better. It was important to learn about the problems related to the implementation of information security solutions in two types of enterprise. Figure 5 shows the categories of problems faced by companies and figures 5a, 5b, 5c and 5d show the causes in a given category.

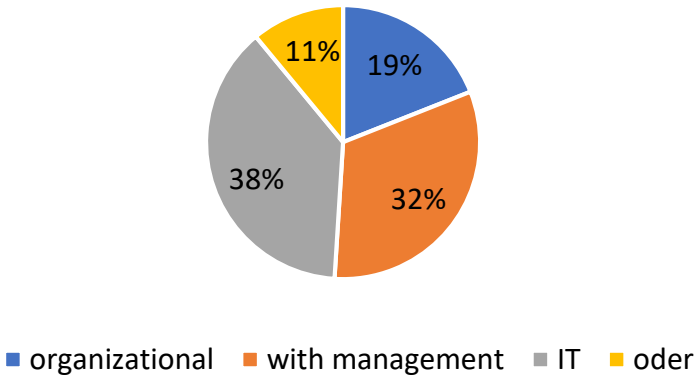
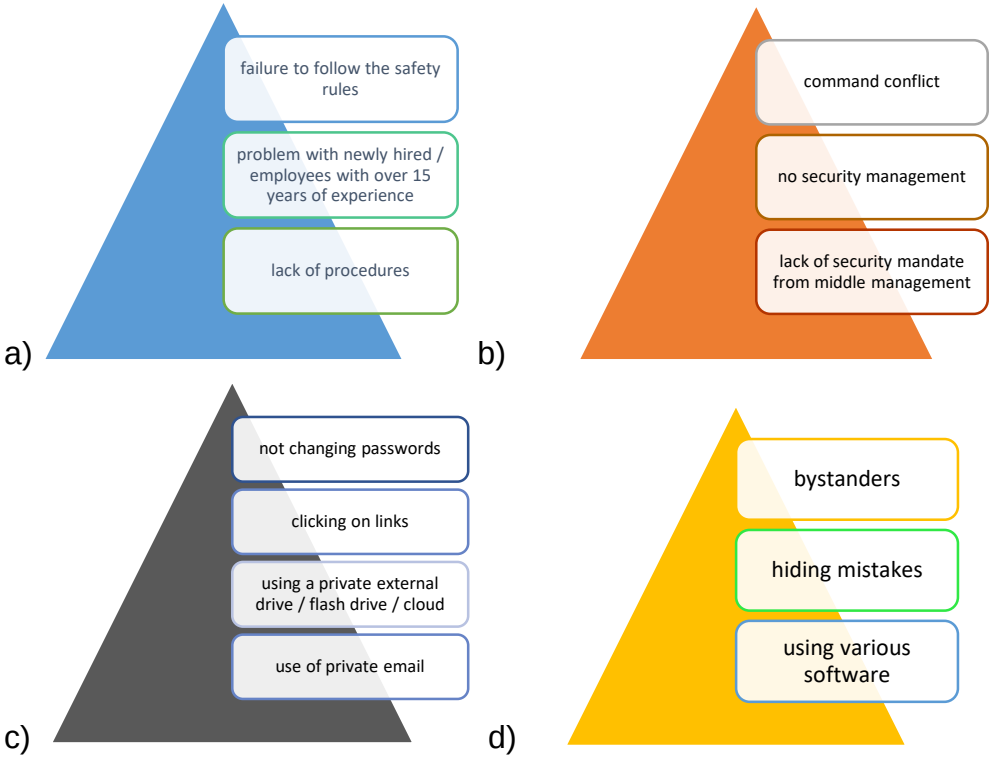


Fig. 5. Causes of problems in implementing information security



a) organizational
b) with management
c) IT
d) order

Fig. 5a,5b,5c, 5d. Categories of information security implementation problems

Demonstration of causes that affect the implementation of security, the awareness of combining all aspects of security facilitates the functioning of the society 5.0 as an employee of the studied enterprise.

The relations between information security and society were also examined 5.0, they are presented in Table 1.

Table 1. The relations between information security and society were also examined 5.0

Relationship between variables	C-Pearson coefficient	Strength of dependence
Understanding safety rules - manifestations of society 5.0	0,91	Very strong
Industry challenges, change of thinking - the tasks of managers	0,78	Very strong
The importance of society 5.0 for the enterprise - manifestations of information security	0,65	Strong
Information Security Challenges - Society Readiness 5.0	0,61	Strong

Only relationships that indicate a strong or very strong relationship are shown. Due to the fact that it was a preliminary, pilot study on a small group of enterprises, the results of this study require discussion. After conducting this study, the authors asked further questions that were to be asked in the actual study (Fig. 6).

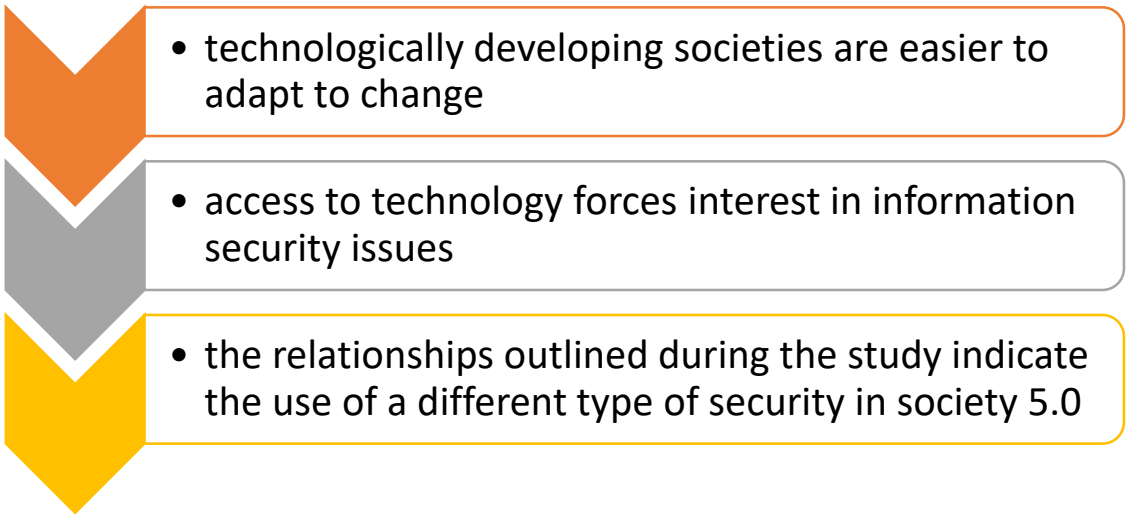


Fig. 6. Questions for further research

The results of the observations and responses to these studies will be published in a future article.

6. CONCLUSION

Changes taking place in enterprises require adaptation in terms of information security. This is a difficult task for enterprises because the mere implementation of IT solutions and the introduction of security rules does not affect the greatest risk factor, i.e. the employee. They pose a threat, often unaware of the need to protect and combine all aspects of information security. The article is an introduction to research on the state of consciousness of employees constituting society 5.0.

REFERENCES

Axelrod, C.W., Bayuk, J.L., Schutzer D. (eds.), 2009. *Enterprise Information, Security and Privacy*, Artech House, Norwood.

Colwill, C., 2009. *Human factors in information security: The insider threat e Who can you trust these days?*, Information Security Technical Report 14.

Griffy-Brown Ch., D. Earp, B., Rosas, O., 2018. *Technology and the good society*, Technology in Society, 52, 1-3.

Horton, G., 2018. *Information politics: liberation and exploitation in the digital society*, Information, Communication & Society Reviews, 21(12).

Lee, A., 2018.*Towards Informatic Personhood: understanding contemporary subjects in a data-driven society*, Information, Communication & Society.

Łuczak, J., Tyburski, M., 2010. *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań.

Stewart, G., 2009. *A safety approach to information security communications*, Information Security Technical Report 14.

Thomas, H., 2018. *Powerful knowledge, technology and education in the future-focused good society*, Technology in Society, 52, 54-59.

Tutton, J., 2010. *Incident response and compliance: A case study of the recent attacks*, Information, Security Technical Report 15.

Żywiołek, J., 2018. *Monitoring of Information Security System Elements in the Metallurgical Enterprises*, MATEC Web of Conferences, https://www.matec-conferences.org/articles/matecconf/pdf/2018/42/matecconf_qpi2018_01007.pdf.

Żywiołek, J., 2016. *The application of value stream mapping method for identifying basic drawbacks and reducing duration of information process in a company,* Production Engineering Archives, 11(2), 36-39.