QUALITY PRODUCTION IMPROVEMENT **2018** No 2(9) pp. 103-112

Justyna Żywiołek[1]

THE THREAT OF PHYSICAL SECURITY INFORMATION IN A MANUFACTURING COMPANY

Abstract: The article presents the results of research on information security issues in manufacturing enterprises. The study covered three large enterprises from the metallurgical industry. The main purpose of scientific observation was to establish elements subject to overexposure and to serve the security of information and to demonstrate which elements are protected and in what way. The conducted research showed considerable deficiencies in physical security, therefore a sheet was introduced for the evaluation of the implementation of the information security management system, which has a real assessment of the progress of implementation work and facilitates zero one-off evaluation of collateral held. The research forms the basis for further research in the field of information security.

Key words: physical threats, information security,

1. Introduction

Security has many definitions. One of them presents security as a state or a process that guarantees the existence of an entity and the possibility of its development. A human being, a social group, a state, an international organization try to influence their external environment and the internal sphere, to remove or at least dismiss threats, reduce the level of fear, anxiety and uncertainty.

Threats may be directed outside and inside, therefore actions taken to eliminate them should be directed with the same force. When attempting to identify the concept of security, it should be objectively stated that defining it is not something easy, because the phenomenon includes several disciplines and scientific specialties. At present, you can find at least a dozen definitions of the term in the subject literature. Each of them points out that security, like peace, is not a state given forever. Dictionary definitions most often define security as the state of a country or a group of states that opposes threats caused by man or nature, eg in a crisis situation. In the dictionary of social sciences, D. Lerner states that in the most literal sense, safety is virtually identical with safety and means no physical danger or protection against it. In other studies in the field of social sciences, one can meet the definition of the concept of security as the ability to survive, independence, identity, and the possibility of development [1]. In the safety theory one should notice the occurrence of two negative phenomena, ie challenges and threats. Challenges generate new situations and needs for which states or groups of countries must adapt their actions in order to achieve a certain state of security. In security research, challenges and threats should

[1] PhD, Czestochowa University of Technology, e – mail, justyna.zywiolek@wz.pcz.pl

be clearly distinguished, because only such an approach can lead to an objective assessment of the safety phenomenon.

Concern for safety manifests itself in all areas of the subject's activity, which is why the structure of the studied phenomenon is in fact identical to the structure of the activity (functioning, existence) of the subject. As part of international and national security, it is possible to distinguish such security areas as, for example, economic, social, military, public, ecological, information security etc. There are also internal and external security - depending on where they are located, where they come from (from inside or outside the entity) opportunities, challenges, risks and threats.

2. Information security in the enterprise

Information security is defined as "information defense, which consists in preventing and hindering the acquisition of data on the physical nature of the current and planned state of affairs and phenomena in its own space of functioning and hindering the bringing of information entropy to messages and physical destruction to data carriers".

At each level of information security management, the main goal is to prevent disclosure. It should be emphasized that too broad an understanding of security may hinder the flow of information (in the state, enterprise, etc.) that are necessary for their efficient and effective functioning.

Information security in a broad sense is understood as a state free of threats, which in turn are described mainly as [4]:

- providing information to unauthorized entities,
- espionage,
- diversionary or sabotage activity.

Information security is also every action, system, method that secures the resources of data collected, processed, transmitted and stored in the memory of computers and ICT networks. Therefore, information security should be understood as a resultant of physical, legal, personal and organizational security as well as ICT.

Ensuring security is a continuous process in which enterprises try to improve protection mechanisms. Recognition of security as a key area of interest of enterprises confirms their actions taken in the face of threats, because these are extremely difficult and expensive, which in many cases may be the reason for their abandonment.

Ensuring security for every user of the ICT system should be one of the priorities. Each company tries to secure its data and information as best as possible. Even with quite large financial and investment expenditures, it is not always possible. In order for the IT system to be safe, all existing security measures should be applied,

staff trained in their proper use, as well as the security of data stored in ICT systems using appropriate security programs.

Security of the ICT system means the use of all available technological safeguards and administrative measures, the purpose of which is to protect the system and data contained in it against accidental or intentional violation or destruction.

Security is also the reliability of the system and the system performing actions in accordance with the user's expectations. However, it is impossible to define the concept of security of ICT systems unambiguously. It probably does not exist (and it is doubtful that it ever was) a completely safe system, because the number of threats and dangers is constantly growing.

The development of the information society, and with it the development of information management and knowledge management, must take into account measures guaranteeing security in the information processing. The creation of documents regarding the legality and security of information processing that will allow the creation of internal regulations and the introduction of protection instruments adequate to the expectations and threats is of particular importance for the effective functioning of the enterprise.

The information security management process can be defined as a set of activities including planning, decision making, organization and leadership directed at the organization's resources with the intention of achieving goals in an efficient and effective manner. The objective of information security management is to achieve and maintain a defined level of security of information processing and to guarantee the confidentiality, integrity, availability, accountability, authenticity and reliability of data. An important element in the information security management process are: resources, threats, vulnerabilities, consequences, risks, hedges and partial risks.

Threats are actions or events that can lead to a compromise of the security of the information processing system. The process of identifying and determining the probability of occurrence should include both accidental and deliberate risks. The threat can be realized only by using existing defects or gaps in the security system. The existence of such gaps or defects in the physical structure of an organization, procedures, management, administration, software, can be used by employees, competitors, hackers and persons or institutions threatening the existence of an enterprise. The direct relationship between vulnerability and resources forces us to perform vulnerability analysis, that is, to study the weakness of the resource.

The consequence is the consequence of an unwanted incident caused by deliberate or accidental action. Determining its magnitude of consequence allows to maintain a balance between the effects and costs of collateral used and is an important element of risk assessment and selection of protection measures. The frequency of appearance of the incident and the amount of losses are not insignificant in the

analysis. The quantitative and qualitative value of incident effects can be defined by the scale according to the criterion:

- costs,
- empirical or adjectival scale of harmfulness.

3. Physical security

Risk is a probability that determines the possibility of a particular vulnerability being used by a given threat in order to cause loss or destruction of a resource, and thus a negative impact on the organization. The risk scenario describes how a given threat may exploit vulnerabilities, thereby exposing the company to damage. The risk is usually determined by two factors: the probability of occurrence and the effect of the event. Every change in resources, threats, vulnerabilities and safeguards has a direct impact on the risk. Risk recognition allows taking actions to reduce or eliminate the negative impact on the organization's activities.

Safeguards are practices, mechanisms and procedures that allow you to reduce risk by [11]:

- protection against threats,
- minimization of vulnerability,
- reducing the likelihood of hacking,
- maintaining the level of security,
- reduction of losses.

Physical security is to ensure the protection of premises, equipment, infrastructure and personnel against the direct action of physical factors and events. However, the security of the IT system is all means that somehow protect against the threat, reduce their consequences and the vulnerability of the IT system. The main security functions of an IT system are: prevention, monitoring, correction, deterrence, detection, awareness and limitation.

The conducted research also concerned protection of physical and IT protection in the surveyed enterprises (Figure 1).

Employees understand the need to secure the server room, they also know where it is located and which rules of special security apply to it. Only 21% of respondents are aware that the data processing areas should be adequately protected. The lowest level of knowledge concerns the safety of carriers. Only 6% of employees know that also CDs, flash memory, external disk or portable computers, palmtops, telephones should be secured.

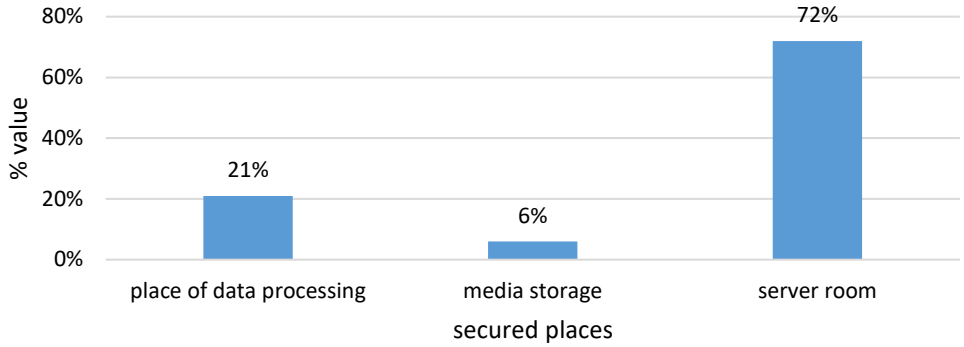

Fig. 1. Secured places in the enterprise

Source: Own study.

In summary, it can be concluded that the implementation of physical security measures takes place in two stages. In the first stage, the level of threat should be determined on the spot, and on the second - appropriate security measures should be selected in specific categories. Such a course of action must be adopted by companies that want to properly build a system of protection of public information, as well as companies already having such a system of protection, but intending to check whether they have applied sufficient security measures. Employee indications regarding knowledge of physical security used in enterprises are presented in Figure 2.

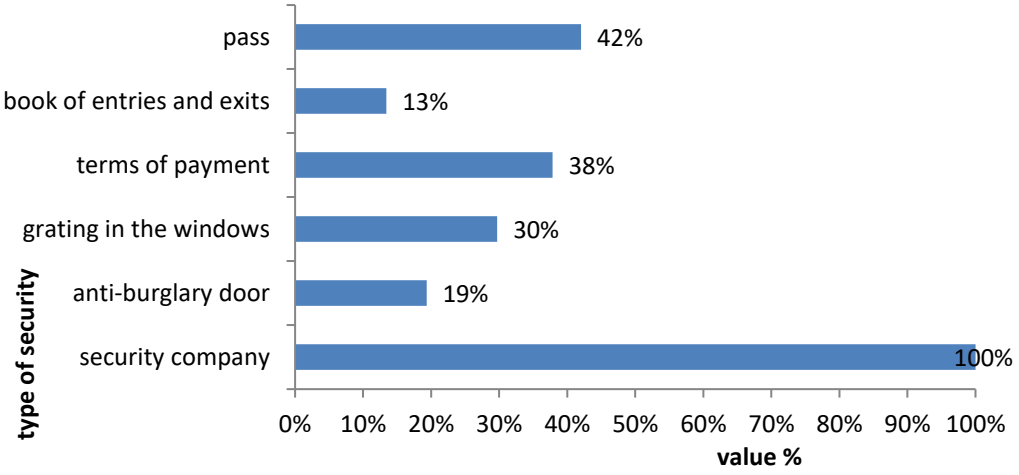

Fig. 2. Types of physical safeguards applied in enterprises

Source: Own study.

Employees of the surveyed enterprises know about the activities of security companies. Care for the entry gates along with the security point was taken care of. Office employees entering office buildings or offices have personal identifiers that are controlled during entry or exit. In companies, there are also entry and exit books, but employees, despite knowing about their existence, do not make entries, e.g. by entering the archive. One of the surveyed enterprises used passes as a form of physical protection. This form, however, with a large number of employees and outsiders who, due to their obligations or being a contractor, had to enter the company's premises, is difficult to implement.

The surveyed enterprises also have a document entitled "Procedures for the security system" defining the manner of implementing processes and activities. Table 1 shows which security procedures apply to the companies covered by the study.

Table 1. Security procedures applied in the examined enterprises

	Ferrostal Gliwice	**HSJ Stalowa Wola**	**WB Zawiercie**
>2015	**movement of people**	–	–
2016-2017	**vehicle traffic**	**movement of people vehicle traffic**	–
2018	–	–	**vehicle traffic**

Source: Own study.

Table 1 presents the procedures that were implemented in the surveyed enterprises and the moment from when they came into force. None of the surveyed entities has IT security procedures, and physical procedures have been limited to personal and car traffic. The level of applicable procedures is very low and requires the creation and implementation of security procedures immediately.

Recognition of the global environment of enterprises allows for determining the elements constituting the environment of their core business. An indication of the environment and elements that should be protected should be made possible and the result reflects the actual state. The global environment of enterprises is presented in Table 2.

The analysis shows that the collateral is not at a satisfactory level. Negligence is long-term and if activities aimed at improving safety are not started, it is possible that the surveyed enterprises will be in danger.

*Table 2. Global environment * of surveyed enterprises*

Security	Ferrostal Gliwice	HSJ Stalowa Wola	WB Zawiercie
physical			
Fence	3	4	2
Entry gate	4	4	4
Concierge	3	3	2
Server Room	4	3	4
Archives	2	3	2
Security doors	1	1	1
Grates in the windows	1	1	1
administrative			
Certyfikowane urządzenia	0	0	0
Certified devices	5	5	0
Cyclic control	1	1	1
Establishment of the ABI	0	0	0
Research of processes	1	3	1
Control of document workflows	1	3	1
Giving protection statuses	0	0	0
Controlling shipments and deliveries	4	4	3

0 - no,
1 - has, but damaged or not used throughout the company
2 - has, but outdated
3 - ma, medium quality
4 - ma, good quality
5 - has very good quality

Source: Own study

Other groups of works necessary for implementation resulting from the scientific observation made during the work on the dissertation were also analyzed. The surveyed enterprises received a project evaluation sheet, in which they had to assess their actual state of enterprises in the area of information security. Obtained information and recommendations are presented in Table 3.

Table 3. Project evaluation sheet

Rating area	Ferrostal Gliwice	HSJ Stalowa Wola	WB Zawiercie
Designation of rooms	No markings	No markings	No markings
The location of the server room and its security	Correct	Correct	Server room secured, but incorrectly located
Separated room for security copies (other than server room)	Lack	Lack	Lack
Security procedures	Partially	Partially	Lack
Alarms, magnetic locks, zone access cards	Partially	Partially	Lack
Shredders, safe	Partially	Partially	Lack
Equipment register	Lack	Lack	Lack
Physical security of computer hardware	Lack	Lack	Lack
Hardware warranty service confirmed by contract	Lack	Lack	Lack
An additional power source for the equipment or a power backup system	Lack	Correct	Lack
Emergency equipment	Lack	Lack	Lack
Cryptographic packages	Lack	Correct	Lack
Illegal software is not controlled	Correct	Correct	Correct
A computer network connected to an external network	Correct	Correct	Lack
Password policy	Correct	Correct	Correct
Transfer of rights	Lack	Lack	Correct
Hard disk controls	Lack	Lack	Brak
Moving files	Correct	Lack	Correct
The determined format of individual documents	Lack	Lack	Lack
Document storage	Correct	Correct	Lack
Safety training for employees	Lack	Lack	Lack

Source: Own study

The observations made show that in the examined enterprises, information security is insufficiently ensured, which may result in data loss and may pose a threat to the proper functioning of the company and may even lead to its collapse. None of the surveyed enterprises has control of hard disks, there are no prepared formats of individual documents, which facilitates their falsification. Business entities do not also maintain equipment registers or have any physical protections, which allows

equipment to be removed or replaced without the knowledge of supervisors. They also do not have emergency equipment, so in the event of any failure, the employee can not perform his duties. After determining what security functions in enterprises and completing the project worksheet, a risk analysis can be performed. These preliminary actions are necessary for the implementation of risk analysis in a correct manner.

The security of business processes comes down to managing information security in every aspect of the organization's operation.

Information technology is developing extremely dynamically, contributing to the emergence of new products and services, but at the same time it is conducive to the expansion of new threats.

4. Summary

The article presents all the necessary elements for the physical security of information. The zones necessary for protection with the list of places that have been well, badly or partially protected in the examined enterprises have been provided. The area covered by the protection and the types of security secured have also been subjected to a breakdown. In order to plan physical information, the global investigations of the surveyed enterprises were examined and a project evaluation sheet for the information security management system was prepared. The presented research results are the basis for further research in the field of information security.

Bibliography

[1] Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń, 2006, pp. 71.
[2] Ciborowski L., *Walka informacyjna*, Wydawnictwo Marszałek, Toruń, 1999, pp. 186.
[3] Czaputowicz J., *System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku*, WNPWN, CSM, Warszawa 1998, AON, Warszawa 2002.
[4] http://encyklopedia.pwn.pl/haslo/3959606/bezpieczenstwo.html (15.05.2018).
[5] http://www.unesco.pl/polski-komitet-ds-unesco/biblioteka/ (21.05.2018).
[6] http://www.zabezpieczenia.com.pl/bezpieczenstwo-it/bezpieczenstwo-aplikacji-biznesowych-czesc-1-bezpieczenstwo-sieci?Itemid=200 (2.06.2018).
[7] http://www.zabezpieczenia.com.pl/ochrona-informacji/teoria-ochrony-informacji-cz-1?Itemid=205 (1.07.2018).
[8] http://www.zabezpieczenia.com.pl/ochrona-informacji/zagrozenia-bezpieczenstwa-informacji-w-przedsiebiorstwie-czesc-1?Itemid=205 (01.06.2018).
[9] Jemioło T., Dawidczyk A., *Wprowadzenie do metodologii badań bezpieczeństwa*, AON, Warszawa, 2008, pp. 46.
[10] Kiełtyka L., *Komunikacja w zarządzaniu*, Placet, Warszawa, 2002, pp. 494.

[11] Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, ISP PAN, Warszawa 1996,
[12] Szymonik A., *Organizacja i funkcjonowanie systemów bezpieczeństwa*, Difin, Warszawa, 2011, pp. 61.
[13] Wójcik A, *System zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001*, http://www.zabezpieczenia.com.pl/ochrona-informacji/system-zarzadzania-bezpieczenstwem-informacji-zgodny-z-iso-iec-27001-cz-1-wprowadzenie. (01.07.2018).
[14] Zygała R., Podstawy zarządzania informacją w przedsiębiorstwie, Wyd. AE we Wrocławiu, Wrocław, 2007, pp. 90.

ZAGROŻENIE FIZYCZNE BEZPIECZEŃSTWA INFORMACJI W PRZEDSIĘBIORSTWIE PRODUKCYJNYM

Streszczenie: W artykule zostały przedstawione wyniki badań dotyczące zagadnień bezpieczeństwa informacji w przedsiębiorstwach produkcyjnych. Badaniem zostały objęte trzy duże przedsiębiorstwa z branży metalurgicznej. Głównym celem obserwacji naukowych było ustalenie elementów podlegających nadzorowi służącemu bezpieczeństwu informacji oraz wykazanie, które elementy są chronione i w jaki sposób. Przeprowadzone badania wykazały spore braki w zabezpieczeniach fizycznych zatem wprowadzony został arkusz oceny projektowej wdrożenia systemu zarządzania bezpieczeństwem informacji, który ma służyć realnej ocenie postępu prac wdrożeniowych, a także ułatwiać zero jedynkową ocenę posiadanych zabezpieczeń. Badania stanowią podstawę do dalszych badań w zakresie bezpieczeństwa informacji.

Słowa kluczowe zagrożenia bezpieczeństwa informacji, bezpieczeństwo informacji, zagrożenia fizyczne

Date of sending the publication to the Editor: 20.06.2018
The date of the publication's acceptance by the Editorial Board: 28.07.2018