Monitoring of information security system elements in the metallurgical enterprises

Justyna Żywiołek[1,*]

[1]Częstochowa University of Technology, Faculty of Management, Poland

Abstract. The article concerns the monitoring of elements of the information security system in an enterprise. The purpose of the research was to determine the reasons for monitoring information flows in the surveyed enterprise. The identification of information flows facilitates information management, empowering individuals to process information and preventing information security incidents. The implementation of information management methods facilitates monitoring the information security status.

1 Introduction

The company should maintain its assumed level of security, which results from the current state of the elements of the security system, that is, the state of resources, vulnerabilities, threats and safeguards. This state is described in the model used for risk analysis, based on the resource model. In practice, it turns out that these elements are subject to changes, which should be constantly monitored, because they affect the overall level of information security and services in the institution. The subject of monitoring activities are changes taking place in the elements of the security system (risk factors), that is in the state of resources, vulnerabilities, threats and safeguards.

2 Changes cause the system's monitoring

Regardless of the reasons for changing the status of elements of the security system, their impact on the assumed level of security for the institution is subject to a thorough analysis, conducted as part of the monitoring process, which defines the types of impact on safety [1]: indirect - caused by significant changes in the systems, detected by the change management process, which take place in the context of their impact on the elements of the security system, direct - caused by changes occurring spontaneously in elements of the security system.

Figure 1 presents typical relationships expressing the impact of various factors on the monitored elements of the security system. Resources are monitored not only in terms of changing their value, but also in terms of changing the security objectives of teleinformation systems (the so-called security purpose may change).

* Corresponding author: justyna.zywiolek@wz.pcz.pl

influence factor - changes	monitored object	monitored parametert
changes in business goals	resources	the attractiveness of the resource
changes in resources or systems	susceptibility	resource weight
change of mind	secured	current performance

Fig. 1. The impact of changes in systems and their environment on the need to monitor the security system.

Threats and vulnerabilities are monitored in terms of changes in their significance, resulting from changes in systems and their environment, as well as in resources [2]. It should be noted that in the case of resources, the decisive factor may be a change in their attractiveness.

In order to maintain compliance of systems with the security policy, it is recommended to constantly monitor [4]: existing security, new systems or services introduced, planned changes to systems and services.

The security attribute is associated with monitoring, that is, accountability and event logs connected to it. Many security measures generate logs that can be subject to statistical analysis, enabling early detection of anomalies, changes in trends and repetitive incidents [5-7]. The institution should appoint people responsible for constantly performing such activities. Event logs are a quite universal mechanism, also used by other post-implementation processes [4, 9, 14].

3 Control of security status through safe data deletion, perimeter control of the facility, document workflow

In many companies, information protection does not work at all, or, as in the surveyed enterprises, it is limited to the use of security in the form of agreements on the confidentiality of information with employees and physical protection for personal and car traffic [3]. Each employee who has access to sensitive information is required to sign an appropriate statement. There are severe penalties for disclosing information that is the subject of the contract. Control of the security system allows to learn about the reasons for the controls [11]. The main reasons for the control, including the people responsible for the controls, are shown in Figure 2.

Almost 70% of documents that are currently created in companies or are created by users are digital [10]. Almost 90% of them, however, will never be printed and will remain only in the memory of computer disks, memory cards and other media, the newer versions of which appear each year on the market [12].

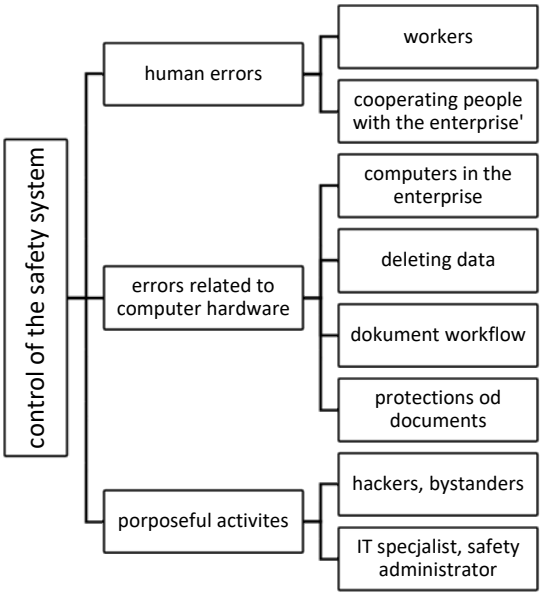


Fig. 2. Reasons for control - diagram Why? Why?

4 Possible control activities of the information security system

In the surveyed enterprises, after the research audit, it was recognized that the greatest threat to the company is the ignorance of employees. For this reason, in addition to the planned audits and trainings, the company decided to be interested in possible measures to control employees' security activities [11, 13].

Conducting research required the use of selected methods of information management. For the design of the information system, one of the methods of information management has been used, counted among the classic techniques of registration of information processes. The Clark chart is a graphical technique of recording and examining the course of the information process, allowing to capture the involvement and activity of the company's organizational units. In addition, it enables detection of unnecessary activities and determination of time losses. The Clark column chart is built from a table of several or a dozen or so columns depending on the number of organizational units. All of the surveyed enterprises have in their structure the following departments: production, logistics, trade, research as well as administration and management for which Clark charts were developed (Figure 3-5).

Functions	The entities						
	Inside					Outside	
	A secretary's employee	Security administrat	Employee	IT specialist	Accountan t	Supplier / seller	Security auditor
Shipping / delivery of a fixed asset						1	
Adoption of the measure	2						

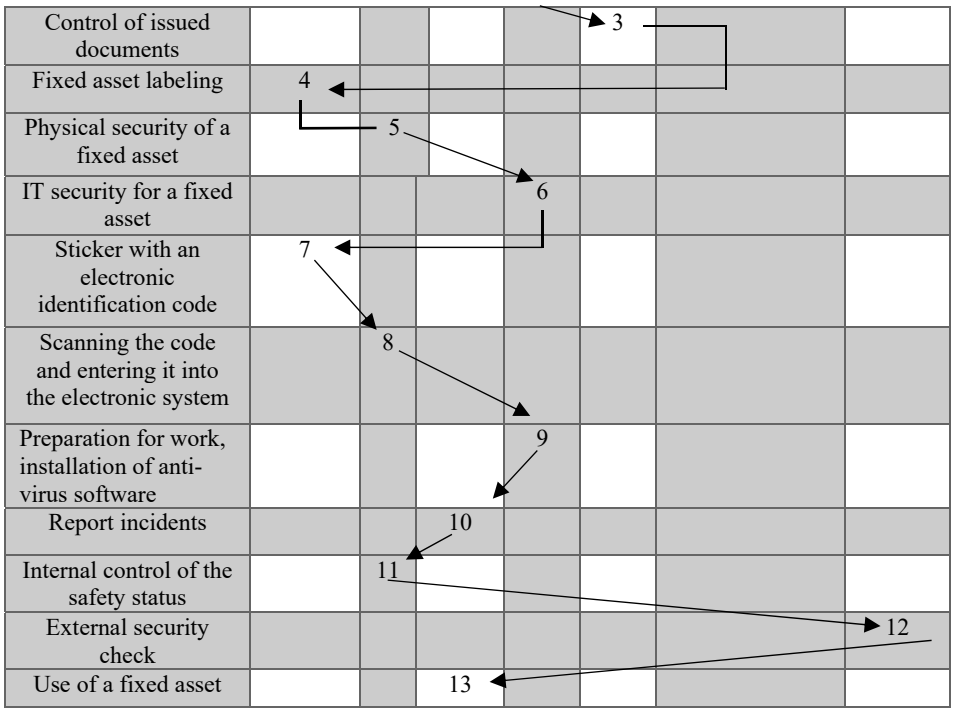
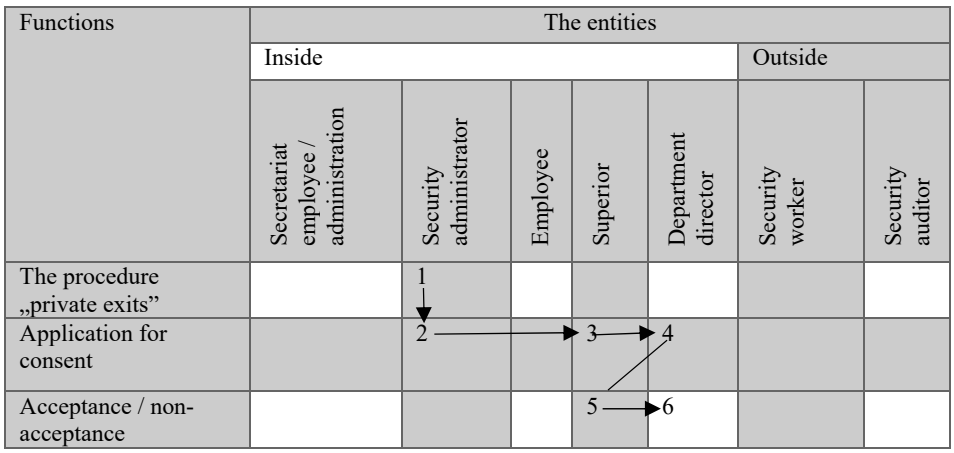


Fig. 3. Clark chart for the procedure of taking fixed assets on the example of a laptop

The Clark chart describing the procedure for accepting a fixed asset is used to design the information process from its delivery to the company until acceptance and use. The individual functions present the stages of the information process, while the entities, divided into external and internal ones, indicate the persons or institutions to whom the information is received, are subjected to processing. Information processing includes the acceptance of information, operations related to its processing, as well as security, if it is required by security rules and sending information for further activities. By dividing the information process into individual stages, the procedures for the information security of the company can be accurately designed. Clark charts also allow you to avoid situations in which elements of the information process reach people who are not well-intentioned or unscheduled in a given information process.



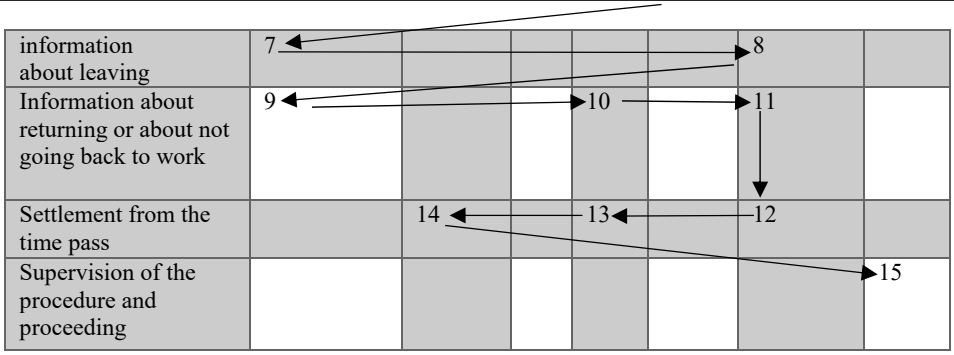


Fig. 4. Clark chart for the employee's output during work

Another element that should be examined in detail to ensure security is incident management. For this type of event, the Clark chart was also developed (Fig. 5).

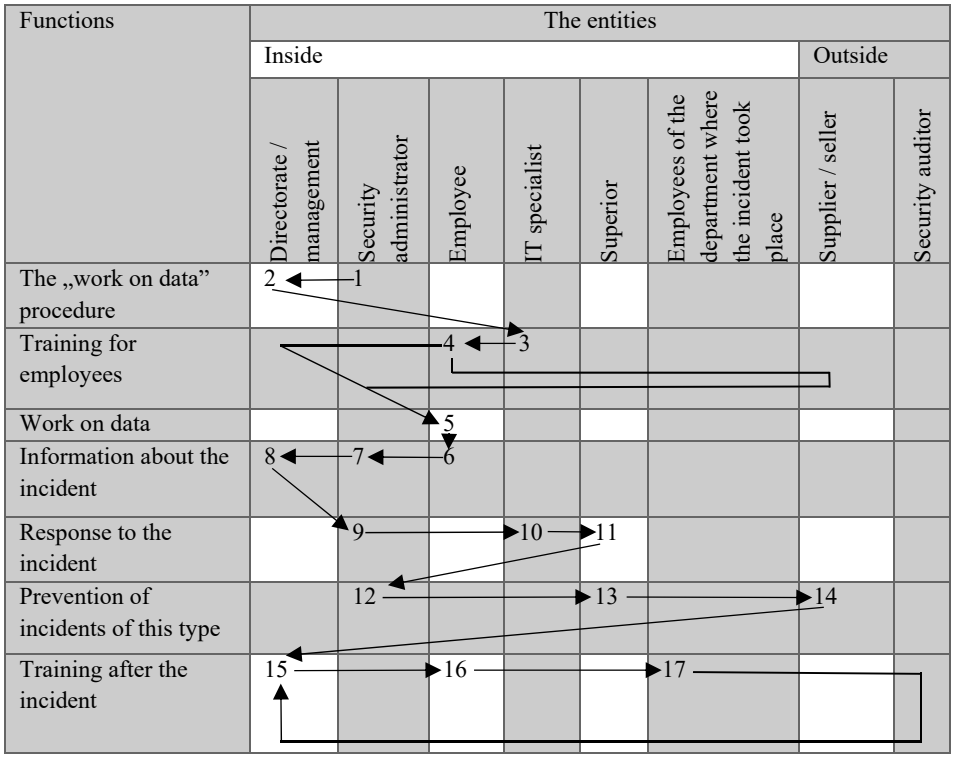


Fig. 5. Clark chart for the possibility of an incident

The occurrence of incidents has a particular impact on reducing the level of information security in the enterprise. Avoiding their occurrence is an important element for security. The developed Clark chart assumes a way of working with data, provides for the possibility of an incident and instructs how to proceed after it. Indication of people informed about the incident allows to avoid further or wider loss of information. The Clark chart also illustrates how important the training activities for employees are during the incidents.
Clark charts prepared and presented are only examples. While designing the information security system, it is necessary to learn about information processes affecting safety.

Summary

It is necessary to take preventive measures in order to be „smarter before harm" and effectively take care of information security within the organization. As in the case of computer viruses, there is unfortunately no recipe for 100% protection against unauthorized information from employees. However, it is necessary to implement certain safeguards leading to minimizing the danger of this type of threats, because they most often result from the intentional action of the employee, not from his ignorance or accident. Appropriate care for information security should be preserved throughout the life of information: from its inception to its permanent destruction.

The information security policy is the key to explaining the actual intentions of the company and people managing information security. This document should be formal and subject to constant supervision, the more so as it is an element of the company's strategy. The assumption of the strategy is the recognition of information processes, their classification and examination of information flows. Implementation of the information security strategy is possible thanks to the use of information management methods. Enterprises have implemented cryptographic keys, a program for sending e-mails to many recipients, and also use electronic signatures. Facilitation of securing results from the use of a clean desk policy, monitoring access to rooms. The solution that brought the greatest effect is the electronic circulation of documents.

References

1. A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej firmie* (WNT, Warszawa, 2007)
2. P. Zou, P. Lun, D. Cipolla, S Mohamed, Safety Science, **98** (2017)
3. A. Lemańska-Majdzik, K. Smoląg, *Role and Importance of Fanpage in Promotion of Products and Services, The Economies of Balkan and Eastern Europe Countries in the Changed World* (EBEEC, Split, Chorwacja, 2016)
4. M. Chałon, *Ochrona i bezpieczeństwo danych oraz tendencje rozwojowe baz danych* (Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 2007)
5. M. Nowicka-Skowron, R. Ulewicz, *METAL 2015* (24th International Conference on Metallurgy and Materials, 1707-1712, 2015)
6. M. Kowalewski, A Ołtarzewska, *Telekomunikacja i Techniki Informacyjne*, **3-4** (2007)
7. K. Liderman, *Bezpieczeństwo informacyjne* (PWN, Warszawa, 2012)
8. A. Brzozowska, D. Bubel, A. Pabian, Procedia - Social and Behavioral Sciences, **213**,992-999 (2015)
9. G. Stewart, Information Security Technical Report, **14** (2009)
10. J. Żywiołek, E. Staniewska, Logistyka, **6**, 382-385 (2012)
11. J. Żywiołek, Logistyka, **6**, 653-658 (2012)
12. J. Żywiołek, Production Engineering Archives, **2**, 36-39 (2016)
13. J. Pietraszek, A. Gądek-Moszczak, T. Torunski, Adv. Mat. Res.-Switz., **874**, 139 (2014)
14. R. Ulewicz, M. Nowicka-Skowron, *26th International Conference on Metallurgy And Materials* (2338-2343 (2017).