International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 07, July - 2017

Engineering of Organization's Security

Martin Halaj
Department of security management
Faculty of security engineering, University of Žilina
Žilina, Slovakia

Ladislav Hofreiter
Department of security management
Faculty of security engineering, University of Žilina
Žilina, Slovakia

***Abstract*— Security is an integral part of any organization as it is directly linked to its survival, development, maintenance of functionality and capabilities. We need to define the factors that directly or indirectly affect it in order to assess the level of its security.**
In this article we aim to identify and to describe the safety factors of the organization and to outline how to divide them. We would like to draw attention to the possible interaction of such factors and its implications. This influence needs to be addressed in the consideration of security factors and assessing the overall level of security.

Keywords*— *Security, Security Factors, Safety Culture

I. INTRODUCTION

The safety or security of organizations is nowadays becoming more important and attentive as people become aware of the importance and security of purpose. By securing and developing security, organizations can protect their assets, their main and supportive activities, improve their work environment and increase profits.

It is important for each organization interested in addressing security issues to be aware of the factors that directly affect its level of security. The security factors of the organizations reflect and evaluate its current state of safety.

The dominant sector of security investigation and its assessment has until now been the property protection, physical and security sector in terms of the impact of security risks of an anthropogenic nature. It is necessary to focus more on the safety of organizations, whether it is production or non-production organization. The object of our investigation is the organization and its security issue. The subject of the investigation is the identification and description of factors that directly or indirectly affect the security of the organization.

II. THEORETICAL BACKGROUND FOR THE INVESTIGATION OF SECURITY FACTORS

In order to examine the safety factors of the organizations, we need to clarify basic information such as what is organization or how to characterize organization´s security. Clarifying ontological aspects related to the organization's security assessment allows the use of a qualitative, explicative method. A comprehensive assessment of the organization's security problem requires examination of these research issues:

- What is an organization, what is the meaning and content of that term?
- What is security, what are the decisive factors?
- How to evaluate organization´s security?

A. What is an organization?

There are several approaches to defining the term organization. H.J. Leawit [1] characterized the organization as a system composed of four subsystems: people, tasks, technologies and structures. G. Morgan [2] characterized five subsystems: strategy, technology, structure, human-cultural and governance.

L. J. Krzyżanowski [3] regarded sources as the basis for defining the organization. According to him, the organization consists of creative sources (people), natural and artificial sources (technology and technology). The organization according to Sedlák [4] is a term to designate an institution, an organized entity, a particular object. In this thoughful meaning, the organization is a whole in which people carry out activity that is aimed at achieving goals.

The most comprehensive definition of organization was submitted by L.F. Korzeniowski [5], stating that the organization is a dedicated group of collaborating people seeking to reach the main goal. The main defined attributes of organization are the common goal, management, corporate culture, organizational structure and synergy of all elements and members of the organization in achieving the goal.

Based on the above definitions, we will regard the organization as material and technological or non-productive objects and technologies (institutions) designed to produce goods, provide services and meet the needs of the population. Such organization can be considered an open, complex, socio-technical, goal-oriented system that is in constant interaction with its environment.

B. Security and security of the organization

The decisive theoretical stepping stone for solving the organization's security is to clarify the term *security*. Finding the answer to the question “what is security” is one of the basic features of a philosophical approach to security. However, defining the notion of security is a major problem, because almost every department of human activity has created its own approach and its own definition.

There is no single, decisive and indisputable definition for security. Security itself is a complex, internally structured, multifactorial and hierarchical phenomenon whose content, structure and functions go beyond the boundary of not only one branch of science (military science, police science), but even entire fields (social, natural) [6]. Security can be defined as a state in which no one or nothing is in danger. It follows that security is subject to and cannot exist without the object of danger, always refers to something or to someone [7].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 07, July - 2017

The security of the organization means a consistent and efficient use of all resources, ensuring the stable functioning of the organization at present and constant development in the future. However, an active approach is needed, particularly in the direction of:

- the continuous detection of proximal (immediate) causes of safety,
- the continuous detection of the ultimate (end) causes of danger to their safety,
- the early establishment of an effective security system to protect its assets.

Gašpierik [8] states that the security of the organization can be characterized as an active use of the security system, task of which is to ensure a security environment for the organization to fulfill its functions and meet the stated goals. For this activity, the organization must:

- characterize its security environment,
- identify possible security breaches,
- identify their significant assets,
- oversee the continuous process of identifying the risks and causes of the danger,
- develop an adequate security strategy in time,
- introduce a comprehensive plan for the protection and safeguarding of security,
- oversee the introduction and development of security documentation.

The organization will be considered safe if:

- it is not a source of danger, it does not endanger itself or its environment (other systems, phenomena, processes and objects),
- it is in such state that it allows its stable and progressive development and fulfillment of the required functions,
- it has sufficient potential to eliminate or to minimize external or internal threats,
- it is capable of immediate reaction to change of its state and environment,
- it can respond to a change in the balance between the threats and the own protective potential (the security system or the protection system).

C. Organization's security system

The organization's security system must be designed to provide effective protection against identified security threats by efficiently arranging and using available forces, technical means and organizational measures.

The organization's security system should ensure:

- development,
- strength,
- stability.

The organization's security system may consist of the following subsystems [9]:

- system of protection of tangible and intangible assets,
- the system of protection of persons (health and safety protection, bodyguarding),
- system of protection of information systems,
- system of technical (technological) safety, including the prevention of major industrial accidents,
- fire protection system,
- system of environmental protection,
- the system of protection of the internal rules in the undertaking,
- the system to protect other security interests of the organization.

III. SECURITY FACTORS OF THE ORGANIZATION

Each reference object, which is also an organization, changes over time or changes its relationships to the security environment. At the same time, the security environment is constantly evolving. Changing conditions around the object affect the security of the object the most. Safety is therefore dependent on the interaction of the following factors:

- threat, that is in an open or latent form in the environment,
- an object with its defensive, protective capabilities, which can be quantified by vulnerability and resilience.

It is important for the organization's security to deal with two groups of security factors:

- external factors including the external security environment, security challenges and security threats,
- internal factors consisting of the internal security environment, the vulnerability and resilience of the organization and safety culture.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 07, July - 2017

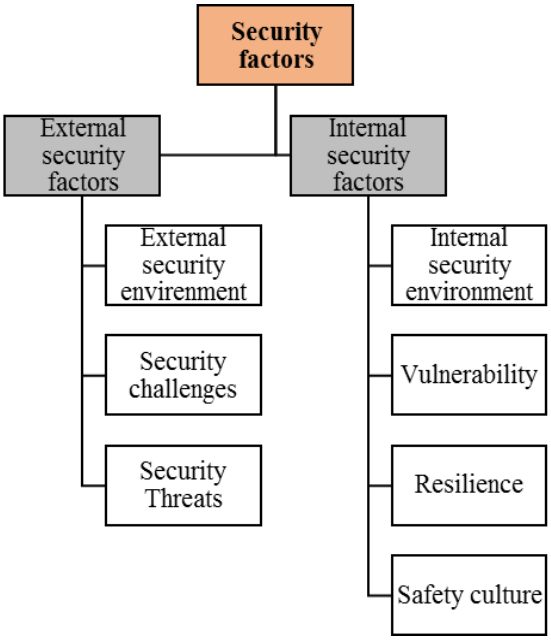

Figure 1 Organization's security factors

A. Organization's security environment

The organization's security environment forms part of the natural, social and technological environment in which it develops in time and space, due to the interactions of actors and the impact of environmental factors, an adequate security situation [10].

The external security environment of an organization can be considered as a space located outside the boundaries of an organization in which factors and processes that have a decisive impact on the organization's level of security are taking place [6]. The external security environment consists of a set of social, natural and technological determinants and other factors that can affect the security and performance of the organization's functions. The organization's external security environment can also be identified as [7]:

- a closer external security environment,
- a remote outdoor security environment.

An internal security environment can be considered as a space located within the organization's boundaries where factors are present, processes that have or may have a decisive impact on the organization's security level are taking place [6]. The organization's internal security environment can be identified and evaluated if the nature of the organization requires it - in case of larger material objects that themselves constitute a more complex, structured structure.

B. Security challenges

Security challenges are changes in the organization's security environment that may have a destabilizing effect on the organization and therefore require an adequate response to them. Security challenges cannot automatically be considered as threats. If an organization responds in a timely and appropriate manner to current challenges, it not only eliminates threats but can increase its level of security as well.

C. Security threats

Security threat is a specific, physically existing object, phenomenon, event or process that has the ability to cause harm. We designate anything that is dangerous to the organization, which could negatively change its security. Security threats are also events and phenomena that may or may occur in a relatively short time and may cause dramatic changes in the conditions of the reference object [11]. Threats may be caused by natural forces or by human activity, they may occur with a certain probability and have the potential to cause drastic changes in the conditions of the organization's existence.

D. Vulnerability

Vulnerability means the property of any material object, technical means, or social subject to lose the ability to fulfill its natural or established function due to external or internal threats of varying nature and intensity. It expresses the result of exposure and sensitivity of the system to negative phenomena and events of anthropogenic, natural or techno-genic nature. Vulnerability is the predisposition of an object or system to disrupt its existence, stability, development, integrity, and / or damage.

Vulnerability has the following aspects:

- external, presented by acts of natural or anthropogenic threat,
- spatial, based on the risk of the organization's dislocation,
- internal, expressing sensitivity and predisposition of organization to injury or damage.

E. Resilience

If vulnerability reflects the system's exposure and sensitivity to negative phenomena and events, resilience means the ability of an organization to cope with negative phenomena and events, preserve its functionality, integrity, persist without harm (to quickly remove damage and losses and restore the normal conditions of its existence).

Resilience of organization can be seen as the ability of an organization to restore its functionality and to reorganize after the occurrence of changes caused by disturbances, external negative influences, events of various character. Resilience can be characterized by:

- resistance to negative effects and events,
- the rate of return to the original state if negative phenomena and events have occurred.

The level of resilience of the organization will depend on the quantity and quality of human, material and financial resources and stocks that can be used to eliminate the consequences of negative phenomena and events.

F. Safety culture

The definitions of the safety culture are unique and differ among authors. Cieslarczyk [12] considered a safety culture as a way of thinking about safety (what is safety, the possibility of expressing safety), the perception of safety and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 07, July - 2017

detection of safety values (how to achieve safety, which techniques and technologies can be used to achieve safety).

We can define safety culture as a set of values, traditions, characteristics and attitudes of organizations and individuals in which the safety of the organizations has top priority, which must be given adequate attention in view of their importance.

Safety culture is a part of the internal security environment of the organization and reflects the perception and assurance of the organization's safety. The safety issues are often subjective due to variety of persistent attitudes, opinions and values of each employee. Safety culture takes many forms and its existence or effectiveness is influenced by many factors, such as norms, values, symbols, conditions, conduction or speech.

To understand the safety culture, it is necessary to identify artefacts, values and assumptions that are part of the culture in terms of safety. Artefacts are most easily traceable, but their interpretation is often challenging. Level of artefact acquires understanding after becoming aware of the values and assumptions [13].

Table 1 Examples of structural elements of a safety culture

Elements	Examples
Artefacts	
Subject	The adoption of Security Policy
Language	No time-loss due to accidents
Ritual	Safety assessment
Behavior	Use of personal protective equipment
Values	Safety first
	Intolerance of safety deficiencies
	Learning from mistakes
Assumptions	The results of negligence are accidents
	Some people are prone to accidents
	In achieving its objectives, it is necessary to look at the risks
	Safety is always possible to improve
	Accidents can be avoided
	Projection device is safe

IV. MUTUAL INFLUENCE OF ORGANIZATION'S SECURITY FACTORS

Organization's security factors can influence each other and thereby change their values. These changes may be positive but also negative for organizational safety. Such factor, in particular, is a safety culture, that directly influences the resulting level of vulnerability and resilience by its values (its level).

Safety culture at the organization level means the acceptance of safety in order to achieve and to ensure organization's safety. There is a particular emphasis on occupational safety and health, and protecting their activities. In the process of creating the organization's security policy, the managers are as important as is the professional competence of employees, which is necessary for finding results in the adverse events in each sectors of the organization. The organization's safety culture is based on the reception and identification of employees with the organization's security policy, as well as on safety behavior within the organization [14].

Organization's safety culture is influenced by:

- adoption of security by senior management,
- allocating sufficient resources to security,
- quality safety documentation and safety procedures,
- strict observance of safety in all sectors of the organization,
- safety trainings and educations,
- readiness of the organization to deal with crisis adverse events assigned forces and means which are permanently accessible,
- regular checks, obstruction and continuously improving of organization's security.

Safety culture affects the safety vulnerability and resilience due to the existence of rules, laws, regulations and standards in the field of security. The introduction and the presence of safety culture in an organization influences the management of the whole organization and behavior of senior management on issues of security and the adoption of security policy.

Enhancing the level of safety culture by creating and implementing security policy, allocating sufficient resources, actively acceding to the management of the organization, observing laws, etc. positively affects the organization and its resilience and vulnerability. It can be noted that by positive influence on the vulnerability and resilience of an organization by a safety culture, increase of the level of resilience and reduction of the level of vulnerability of the organization can be achieved. However, if the level of the culture of safety is not sufficient, the organization can very hardly increase the level of resistance and reduce the level of infertility. There may even be an adverse (negative) effect for the organization (increase the level of vulnerability and reducing the level of resistance).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 07, July - 2017

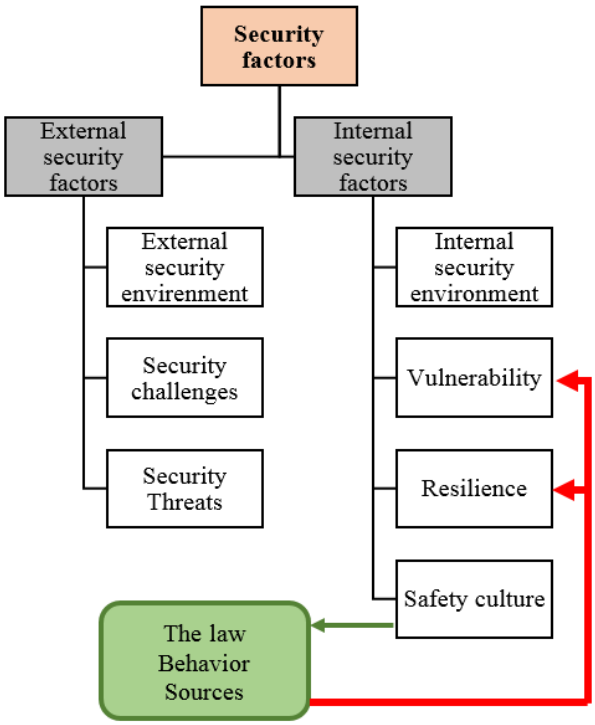

Figure 2 Influencing the security factors of the organizations by safety culture

During the organization's security assessment, we rely on the mutual iteration of internal and external security threats and protective (defensive) features, capabilities and options parameterized through a vulnerability and resilience factor. It follows that the safety culture influences the overall security of the organization by its impact on vulnerability and resilience. Therefore, this safety culture needs to be given the necessary attention.

V. CONCLUSION

Organizations should focus their attention on safety, in particular to protect the life and health of their employees, to protect their property, to protect the environment in order to meet the legislative requirements. Security must be one of the main strategies of the organization which should be given adequate attention to, and organizations should regularly allocate sufficient resources for its retention.

Organization's security factors such as security environments, threats, vulnerabilities, or safety culture are important for organizations, enabling them to determine their current security status and to identify weaknesses in order to develop security and raise its level. A safety culture is a security factor of the organization that can directly influence some of the remaining security factors and directly alter the security level of the organization. The organization's choices are to take the necessary measures to increase the level of security culture. It should be noted that an organization cannot provide the required level of security while ignoring its security culture.

ACKNOWLEDGMENT

This article has been supported by institutional grant project of the Faculty of security engineering at University of Žilina (IGP201702).

REFERENCES

[1] March, J. (1965). Handbook of Organization. Chicago: Rand Mc Nally.
[2] Morgan, G. (1997). Obrazy organizacji. Warszawa: PWN.
[3] Krzyzanowski, L. (1999). O podstawach kierowania organicajami. Warszawa: PWN.
[4] Sedlák, M. (2001). Manažment. Bratislava: IURA EDITION.
[5] Korzeniowski, L. F. (2010). Menedżment . Podstawy zarządzania. Krakow: EAS.
[6] Hofreiter, L. (2006). Securitológia. Liptovský Mikuláš: AOS.
[7] Hofreiter, L. (2015). Manažment ochrany objektov. Žilina: EDIS.
[8] Gašpierik, L., Reitšpis, J., & Selinger, P. (2011). Bezpečnosť podniku – významný činiteľ súčasnosti. Krízový manažment. Žilina.
[9] Belan, L. (2015). Bezpečnostný menežment. Bezpečnosť a manžérstvo rizika. Žilina: EDIS.
[10] Hofreiter, L., & Matis, J. (2010). Komplexná metodika hodnotenia bezpečnostného prostredia. Liptovský Mikuláš: AOS.
[11] Hofreiter, L. (2013). Ochrana objektov kritickej dopravnej infraštruktúry. Žilina: EDIS.
[12] Cieślarczyk, M. (2011). Kultura bezpieczństwa i obronności. Siedlce: Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego.
[13] (2010). Kultura bezpečnosti v jaderných zařízeních: Návod pro použití při zvyšování kultury bezpečnosti. Praha: Státní úřad pro jadernou bezpečnost a Výzkumný ústav bezpečnosti práce.
[14] Halaj, M. (2016). Kultúra bezpečnosti ako aspekt bezpečnosti organizácie. Współczesność i perspektywy rozwoju badań nad bezpieczeństwiem (s. 35-44). Kraków: EDIS - vydavateľstvo ŽU v Žiline.