Proposal of Model for Security Management Integrated System

Lukas Kralik, Roman Senkerik

Abstract—Security passes through all management levels of the organization and must cover all areas of the organization activities and must affect the operation of security mechanisms. Currently the requirements for security are increasing and within large amounts of these requirements and their security-related obligations individual links and relations are fading. A number of activities are unnecessarily multiplied and repeated. Thus this issue makes (already expensive) security to be more expensive. The way out of this situation is the integration of security activities in order to eliminate duplication and create a comprehensive integrated security system.

Keywords—security, security management, organizational structure, integrated security system.

I. INTRODUCTION

The main purpose of the security system is to ensure the safety organization in all possible aspects. This system is characterized by dynamic and constant influence of a large amount of variable factors on the processes of this system. Basic and simultaneously the weakest elements of the security system is people (own or other employees), technology in the form of material resources, a network of organizational relationships in the form of regime measures and last but not least information.

In practice, we usually understand under the concept of company’s security system correctly created security policies that are implemented into the daily running of the organization which making it as a foundation of functional safety and security management system of the company. Sufficiently secured organization's assets against damage or destruction are an essential element of security management. With regard to the increasing number of attacks on the organization's assets, it was necessary to establish a security system for the organization [1].

Such a system is designed to help faster and more efficiently to focus on individual sectors of safety and security with regard to safety and security aspects, which are essential for the organization. Underestimating security system leads to serious disruption of the daily operations of the company. The consequences can be serious for the company and its management. The company's security management system given by means of the set of objectives, strategies and policies hierarchically allocates the area of security solutions from the corporate level to the individual protected areas (for example human resources, information security, etc...). An extension of security system represents the security policy. Two parts create the security system. The first part consists of operational and technological security and the second part is the classic security [2].

The security measures of information, physical and human resource security pass through both of these parts. Security of human resources represents the basis of the security system of the organization, since it includes the human factor issues and the process of security consciousness, which means accountability and shared responsibility for security. The problem at present is how to rationally and effectively manage elements of the security system.

Currently the usage of modern approaches, decision support systems (for example based on ITIL framework) [3] - [6] are the main open tasks in the integrated company security systems, together with the development of more robust and effective systems dealing with the information security [7], [8].

II. EVALUATION OF THE CURRENT ORGANIZATION'S APPROACH TO SECURITY MANAGEMENT

The quantity and diversity of laws, regulations, technical standards and methodologies together with the extension of the security field causes lose relations and links between individual areas of security. Security takes many forms for different protected systems. As a result, it leads to the fact that there are fragmented objectives, resources, and practices in the field of security, which lowers the security standard. Duplicity, disunited terminology and uncovered spaces are result of the low integration of security processes within their companies. Activities associated with the security management of the company are carried out separately within each functional department, which leads to inefficiency. Various experts ensure lot of activities, which are similar or identical. This fact causes that expensive security is even more expensive than it is necessary (See Fig.1).

Security sectors that in the opinion of company management pass through the entire company and require
unified management are entrusted to the security department. Other security areas are entrusted to the individual organizational units. In many companies, this disunity affects the main (top) management from the perspective of the organizational integration of individual departments dealing with security issues, and also from the perspective of communication and cooperation between these departments and their managers. This approach to security management brings another problem, which is disunity of used terminology.

Fig. 1 Separate security management in company

Fundamental flaws in companies' approach to security management are:
- Separate management of individual security areas, which entails:
  - Fragmentation of objectives, resources, procedures that are related to security.
  - Duplication of activities.
  - Inconsistencies within terminology.
  - Inconsistent methodology.
  - Insufficient coordination and cooperation of management associated with the low integration of management processes in security areas.
  - Fragmentation in security management.
  - Decreased ability to respond to security abnormal situations.
  - Higher security costs.
- Absence of comprehensive legislation, which clearly define the individual security areas.
- Absence of legislation defining the type and method of maintaining security documentation for all security areas.

III. A COMPREHENSIVE APPROACH TO THE PROCESS OF ESTABLISHING SECURITY

The objective of the comprehensive approach to the process of establishing security is not to have the best possible security. But to have set a combination of security measures, which cover the main threats and reduce risks to an acceptable minimum. A comprehensive approach to the process of establishing security is a way to minimize mentioned consequences of separate solutions, especially of separate security management for individual security areas [3] - [6].

It is very important for this procedure not to place too much emphasis on one element of security solution that would be at the expense of other security elements. For a comprehensive approach to the process of establishing security it is necessary to ensure that the solution is always balanced and solid. At the same time, security costs must be proportionate to the value of the protected assets or the level of risk. This is because investments in security are rightfully increasing, and therefore they need to be properly, functionally and efficiently spent.

Security passes through whole company and must be correctly managed. Its underestimation may cause serious damage to the company’s functionality. Therefore, it is necessary that the decision to establishing security are based on the decision of the top management that wants to deal with security and mainly on the decision about correct approaches. Top management of company must make decision what they expect from security, how will be the security management implemented, how to evaluate current level of security in company and how will be formulated the future development of security management in company. This activity does not provide at first sight concrete results. There is no immediate visible result and usually does not noticeable any significant improvement in company’s performance. Vice versa, often in
establishing security, for example the risk analysis, so the disorders in company are shown. In addition, some steps in establishing security may work of company rather slow down.

The expected benefits of a comprehensive approach to the process of establishing security of company are:

- Consistency of management and security processes;
- Consistency of control, security and crisis documents;
- Lower the cost of implementing security in comparison with individual solutions,
- Creation of united methodological environment,
- Integrated documentation system of company’s processes.

A. Integrated Security Management System

The result of a comprehensive approach to establishing security is an integrated security management system. Integrated security management system is a set of leadership skills, organizational structures and processes which objective is security of company. The main prerequisite for the success of organizational structures and processes is effective communication between all stakeholders and based on constructive relationships, united terminology and shared support of defined objectives. Top management of company must make decision what they expect from security how will be security management implemented, how evaluate current level of security in company and how will be formulated future development of security management in company. Company must establish responsibility for security as a separate part of management. Security should not be part of other roles that lack the powers, responsibilities and resources to enforce it. Integrated security management system organization must implement the basic relationships between the different areas of security. Process of security management must be perceived as a solution of complex problem in which it is necessary to manage not only the security of company as a complex, but also its each aspect.

Fig. 2 Relations and responsibility in the organizational structure

B. Model of integrated security management system from the perspective of the organizational structure

The mostly utilized current approach for security management, which is characterized by separate management of individual securities, does not allow implementing the model of integrated security management system. Figure 2 shows a proposal of model that demonstrate the basic components of an integrated security management system from the perspective of organizational structure, including the
responsibility for their implementation and mutual relations. In the context of establishing of an integrated security management system in the company, there must appear new units in the organizational structure. Names of organizational structures and departments are not essential. What are important: their job; responsibilities and competence in design, implementation and operation of an integrated security management system.

Security team is responsible for managing the assets of the company. A condition would be that members should have sufficient experiences in the security management area and be able to issue and manage tasks and some of them have to directly perform. It would be a top unit of the company in issues of security management, which should provide conditions for:

- Risk analysis.
- To develop a plan for the creation and approval of documents in connection with the security management system.
- Be responsible for the content of the documents and provide their approval by top management.
- To solve problems, which arise in the context of an integrated security management system and has crossed the framework of competencies for security planning team.

The team should be build by internal employees. And the head of this team should be known as a security manager. Team size would depend on the size of company and the nature of the production program.

The team for security planning should be a specialized team that would be responsible for the provision and implementation of security management system in company. Its members must have qualified information and knowledge about the company's assets and their protection. The task of this team is assessing different aspects regarding the protection of assets and resolve conflicts that might arise between organizational units of the different security sectors. The head of this team is the same person as for security team - the security manager. The main condition for the functioning of team for security planning is fact that all the heads of each security sector must be on the same management level to promptly and competently respond to arising problems.

Incident team is only temporary team that will be used only for solving of security incident. Team members must be experienced employees in security sectors and there must be represented all security sectors. One of team member must be the head of department, where the incident occurred. Afterwards, depending on the nature of the incident, another team member will be an expert on specific problem. And last but not least, members of the team will be heads of departments that are affected by incident. Such an incident team will be appointed by main (top) security team. The head of this team can become a person of top management however it is depending on the nature of the incident. Furthermore for the direct solving of the incident, an external specialist or consultant should be used. Nevertheless such procedure should be realized only in cases, when the incident danger grows or has already arisen into a crisis situation.

IV. CONCLUSION

This paper represents the complex overview current mostly used approach for company’s security systems. Furthermore it presents the proposal of complex integrated security model. Model of integrated security management system from the perspective of organizational structure is based on:

- Classification of responsibility for security to the level of top management of company.
- Allocation of responsibility for the security and secure its support.
- To ensure the effectiveness of integrated security management system in the form of its control and approval.
- To create a new organizational unit - security department.

Model of integrated security management system from the perspective of organizational structure will allow interaction between the individual security sectors as well as risks management based on indicators for reducing the impact of any threats to an acceptable level and optimize investment in security.

REFERENCES