ANNALS of Faculty Engineering Hunedoara
International Journal of Engineering
ISSN: 1584 - 2673

OPTIMIZATION OF SECURITY MANAGEMENT OF INFORMATION SYSTEMS IN ENTERPRISES

[1] Samer KHOURI, [1] Denisa AL-ZABIDI, [2] Monika OROSOVÁ

[1] The Technical University of Košice, Faculty of Mining, Ecology, Process Control and Geotechnology, Košice, SLOVAKIA
[2] The Technical University of Košice, Faculty of Mining, Ecology, Process Control and Geotechnology, Košice, SLOVAKIA

Abstract:
Information and means of its processing are today the most important actives that are at disposal for subjects. The possibility of misuse increases with intense development of information systems. Because the development in this area is very fast, competitive environment is becoming more aggressive and malfunction of information systems can cause irreplaceable damage. In this regard the need to solve the problem area of optimization of information security, or control of information systems. Security management of information systems represents a process by help of which dangers can be analyzed, controlled, supervised and limited.
Keywords: security management, optimization, enterprises, information systems

1. INTRODUCTION

Informations are one of the most important actives that are at disposal for enterprises and therefore the enterprises are interested in their protection. Loss of data, loss of information, loss of business secrets, malfunctions of information system all represent high risks to operation and development of the enterprise and therefore it is necessary to search for optimization of security of information systems with the aim to efficiently control these risks with the aim to lower probability of their occurrence and lower the possible damages.

The main aim of the article is to define the term of information security, classification of enterprise actives and analysis of security risks with clarification of the process of security management of information systems and presented findings resulting from a survey of information security in Slovak republic.

2. INFORMATION SYSTEM OF ENTERPRISE AND DEFINITION OF ITS ELEMENTS

The enterprise information system is a file of hardware and software equipment, data media, data and personal that is used by the given subject to management and transfer of information. These material and immaterial objects are selected on purpose and mutually interconnected for the purpose of gathering, exchange, processing, storage, generation and distribution of information and data in a defined structure in defined time to obtain execution of decisions, support of decision making process, information and communication. The material elements of the information system are:

- user technologies, mainly computation technologies (PC, servers, disk fields),
- communication technologies (cables, active and passive network elements).

The value of these actives is set mainly by their acquisition value. Immaterial elements of the system are represented by software and data. Here belong mainly:

- operation systems,
- applications,
- program tools for administration and control of the information system,
- database, which is the main value of immaterial actives

3. THE TERM OF INFORMATION SECURITY

With rapid development of information systems, the possibility of their misuse also grows. The more rapid development in the area is, the more aggressive the competitive environment becomes and

in this setting even a short malfunction of an information system can cause irreplaceable damage. Enterprises lose high financial means because of random malfunctions, loss of data or random incidents. The damages form deliberate actions of employees or third parties are also considerable.

The need to solve the area of security of information systems is therefore ever more important. A new discipline in the area of management is developing – the management of information security. By information security, we mean protection of information in time of their creation, processing, storage, transfer by means of logic, technical, physical and organizational measures to prevent the loss of security, integrity and accessibility. It is not possible to secure full security of an information system and the emphasis on closure to high security is financially very demanding. By efficient functioning of security management of information systems the risks can be optimally eliminated.

4. DEFINITION OF THE TERM INFORMATION ACTIVE

Regarding the information systems and their security, the important term is information actives. It is a material or immaterial object that deals with functioning and creation of an enterprise information system. The information actives can be classified into three main groups:

a. **data and documentation actives,** databases and data files, data and information, system documentation, user manuals, operating procedures, contracts about replacement approaches used in case of malfunction of supplied services or system, archived data. Data structures represent the greatest value of the system. Their loss is only very hardly assessed and their value can change over time rapidly;
b. **software actives,** this is applications software, systems software, development tools and subsidiary programs, source libraries and libraries of executive programs;
c. **physical actives,** here belongs the computer equipment (processors, monitors, modems, laptops, etc.), communication equipment (routers, faxes, etc.), magnetic media (tapes, HDD), other technical equipment (power units, climatization units, UPS), furniture, etc.

5. RISK ANALYSIS OF AN INFORMATION SYSTEM

Before beginning of the analysis of risks, the organization should have finished strategy for this analysis. Its parts (methods, techniques, etc.) should be documented in security politics of the whole organization. The organization should have prepared means and criteria for selection of risk analysis methods. By selection of appropriate methods of risk analysis it should comply to security standards accepted in Slovakia (STN ISO/IEC TR 13335, STN ISO/IEC 17799) and other countries of EU (BS 7799, IT baseline Protection manual). (Khouri et al. 2009)

The risk analysis is the basic assumption of creation of efficient system of protection of information systems. The aim of the risk analysis is to identify and evaluate dangers to which the information system is exposed, so that the protection measures could be taken. Risk analysis identifies dangers and their risks that have to be accepted or corrected. In the context of security of the system, the model of risk analysis includes (Figure 1):

- identification and evaluation of actives,
- dangers,
- vulnerability,
- identification and analysis of risks,
- selection of protective measures.

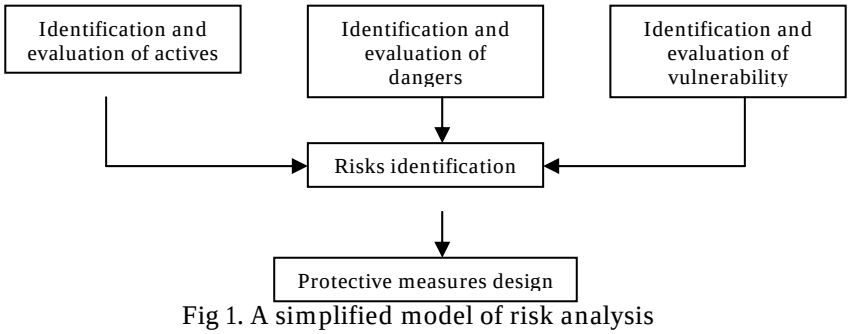

Fig 1. A simplified model of risk analysis

Risks are evaluated from the point of view of possible impact caused by disruption of trustworthiness, integrity, accessibility, etc. With regard to the type of organization, complexity of information systems and output demands, it is possible to choose from four basic approaches to risk analysis:

- **Basic approach -** As the first possibility, the enterprise should apply basic security of all IT systems by selection of standard protective measures. Detailed evaluation of dangers, vulnerability and risks is not necessary in this case. Everything that has to be realized is selection of the parts of protective measures relevant to the given IT system.
- **Informal approach -** Represents a pragmatic risk analysis. It is not based on structured methods, but it uses knowledge and experience of specialists from practice.
- **Formal approach** (the detailed risk analysis) - Includes deep identification and evaluation of actives, evaluation of dangers for these actives and evaluation of vulnerability. The results of these activities are then used for evaluation of risks and identification of protective measures.
- **Combined approach -** It is based on the fact that at first a general risk analysis for all IT systems is executed that is centered on value of actives of every system. The systems that are identified as important for operation of the enterprise and are facing high risks a detailed risk analysis should be done. For other IT systems the basic approach should be chosen.(Khouri et al. 2009)

It is necessary to analyze risks in the following situations:

- to find the actual state of safety of enterprise information system,
- in case of incursion of the system of information safety in the enterprise,
- in case of re-structuralization of the,
- for satisfaction of demands of auditory companies,
- before taking safety measures,
- as a part of preparation for inclusion of foreign capital,
- in case of legislative order,
- in case of high doubts about security of information, etc.

Among main contributions of realization of risk analysis belongs:

- finding the actual knowledge about information safety in organization by an independent site – setting the actual level of security of the information system,
- identification of risks and weak points in security that endanger key functions and actives of the organization,
- considerable increase in the level of safety of system by implementation of the proposed means,
- obtaining of foundations for decisions of management about allocation of investments into security of the information system.

6. MANAGEMENT OF SECURITY OF INFORMATION SYSTEM

The security of information systems can be defined by three basic demands:

- trustworthiness, protection against leakage of information,
- integrity, protection against unauthorized modification,
- accessibility, protection against unauthorized refusal of services or inability to supply information.

These basic demands are mutual for all information systems. Their balance is dependant on demands on the particular system. For example the trustworthiness will be over integrity in army systems, the integrity of data will prevail in broad information libraries etc.

Vulnerability of information systems represents a deficiency or weak spot of the whole security system that can be misused by a danger in the way of loss of information actives. High damages can be caused by disintegration of trustworthiness, integrity or accessibility of delicate data and information, therefore these require higher protection. We speak mainly about personal information (telephone numbers, addresses, etc.), data protected by law about state secrets and delicate commercial information – data about accounts, contracts, client databases, etc.

Management of risks in information systems represents a process by which it is possible to set control and limit influence of random events. It contains identification, analysis and evaluation or assumption of risks. The evaluation of risks is process of evaluation of dangers acting on information system of the enterprise with the aim to express the level of risk the system is exposed to. Correct risk evaluation can find out if the security measures are sufficient.

7. A SURVEY OF STATE IN THE INFORMATION SOCIETY

The survey of state of information society was ongoing in the year 2008. It was aimed on a representative sample of middle and large comanies in Slovak republic, covering all vertical segemnts. In an anonymous survey, they responded to 59 detailed questions from the area of information security that were divided into 11 thematic groups. From 826 companies, 205 sent back the filled questionaire and 187 of them were put into processing. The survey was done by Ernst &

Young together with the magazine DSM – data security management and national security office. In the figure 2 is distribution of respondents according to employees count.

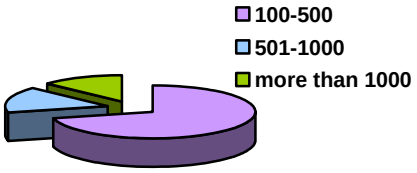

Fig 2. Distribution of respondents according to employees count

The results of the survey have shown, that the companies value factual knowledge, IT technologies and flexibility by their security employees, on the other side the mainly miss the knowledge of financial control and abilities to efficiently communicate with leadership. Nearly a third of all employees responsible for information security earn more than 1800 €, what represents a significant rise against the year 2004. (SITA 2009)

Power loss belongs to the greatest dangers. Furthermore it is SPAM and hardware malfunctions. However it is bewildering that even due to the existing dangers, 55% of the companies do not have worked out plans of functionalities recovery and two thirds of the companies have not worked out any risk analysis of the information system, what also represents a negative trend. Also one third of the companies does not use a system of monitoring of security accidents and more than a quarter does not have any formal approaches in this area worked out.(PSIB SR`08 2008)

In the figure 3 are main obstacles in implementation of information security in SR

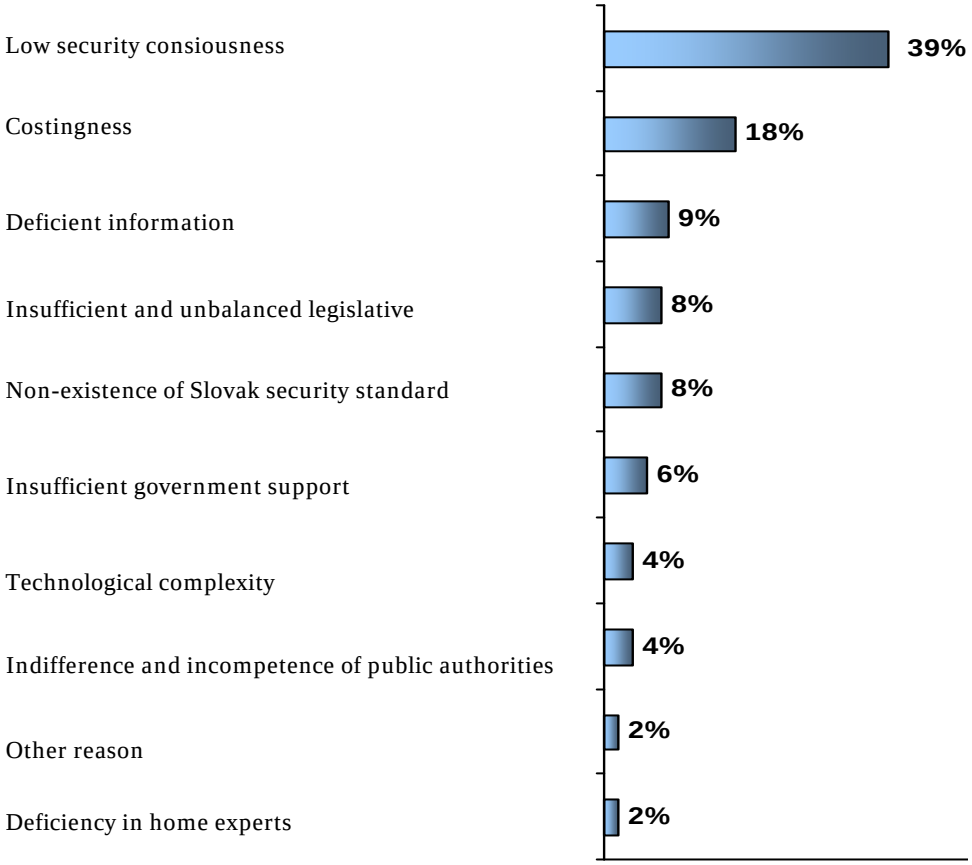

Fig. 3. Main obstacles in implementation of information security in SR

Tab 1. Average financial costs of the most important security accidents

Malfunction of software	18 000 €
Malfunction of WAN	8 300€
Hardware malfunction	4 000 €
Computer virus	3 700 €
Natural disaster	2 800 €
Theft of equipment	2 300 €
LAN malfunction	2 000 €
Electric current loss	1 700 €
Administrator or operation mistake	1 100 €
User mistakes	250 €

The results of the survey show that most of the companies is stopping investments into new IT solutions and is functioning only in upkeep regime. The main priority in the area of their information security is solution of the identified known problems. The most important security challenges in the past period was transfer to euro and implementation of new operating systems

8. CONCLUSSIONS

Use of information systems and technologies hasn't been a fashionable or prestigious feature for a long time, but a method of survival of many companies. Technological system and the corresponding personal, physical and administrative imperfections of data processing are used by many dangers. These are further transformed into higher or greater risks dependant on the value of information actives and their usage in the company coupled with probability of occurrence. The risks then transfer into bigger or smaller security incidents that every day attack security of information of the company.

This means that the company receives smaller and bigger invisible blows that do big damages. Therefore the area of security systems management has emerged. It is a complex information protection, where also the physical security, object security, personal security and administrative security belong.

REFERENCES

[1] *Cehlár, M., Mihok, J., Kyseľová, K., Bohušová, V. 2005. Informačný systém ťažobného podniku a jeho vplyv na zhodnocovanie ložiska. In: Uhlí-Rudy-Geologický průzkum. vol. 12, no.4, p. 24-28. ISSN 1210-7697.*

[2] *Cehlár, M., Cehlárová, I., Khouri, S. 2009. Model riadenia podniku v kríze. In: Doprava a logistika. mimoriadne č. 6: 121-124. ISSN 1451-107X.*

[3] *Khouri, S., Al-Zabidi, D., Alexandrová, G.. 2009. Manažment bezpečnosti informačných systémov a analýza jeho významu. In: Informatika a automatizácia v riadení procesov: 5. vedecká konferencia: Zvolen, 10. september 2009. Zvolen : Technická univerzita vo Zvolene. s. 139-143. ISBN 978-80-228-2029-5.*

[4] *Khouri, S. 2009. Analýza bezpečnosti informačných systémov organizácií. UNIFOS 2009 (Univerzitné informačné systémy) Slovenská poľnohospodárska univerzita v Nitre, medzinárodná konferencia 25. – 27. november: 140-144, ISBN 978-80-552-0309-6.*

[5] *PSIB SR `08, Erst&Young, NBÚ SR, DSM – data security management, TATE International Slovakia, 2008. Prieskum stavu informačnej bezpečnosti v SR 2008. Aveilable from Internet: <http://www.dsm.tate.cz/cz/psib-sr-2008/>.*

[6] *SITA, 2009. Informačná bezpečnosť je pre väčšinu firiem dôležitá [online] [accessed 22 January 2009]. Available from Internet: <http://www.itapa.sk/index.php?ID=6609>.*

ANNALS OF FACULTY ENGINEERING HUNEDOARA
– INTERNATIONAL JOURNAL OF ENGINEERING