Protection of Information and Communication Systems

Jiří Barta, Veronika Sadovská, Albert Srník, and Jiří F. Urbánek

University of Defence, Kounicova 65, 622 10 Brno, Czech Republic
{jiri.barta,veronika.sadovska,albert.srnik,
jiri.urbanek}@unob.cz

Abstract. Awareness, education and protection of organizational information secure environments are currently highly serious and relevant topics. The paper deals with the perspectives and possibilities of "new approaches" to the protection of information and communication systems and nets as a part of Czech Republic critical infrastructure. It means that selected technologies are used, considering new perspectives to interoperable management training and education. The first part of this paper is focused on the current state of organization management information systems in Czech Republic. The second part concentrates on the possibilities of new technologies application and computer-aided tools, protecting information & communication systems and other assets.

Keywords: Interoperability, Security environment, Assets, Communication and information systems, Safety.

1 Introduction

From the distant past to the present, the people have to satisfy their subsistence needs that closely relate to their existence and to a preservation of their culture and assets. The human society was changing all the time, especially at the scientific and technological platforms. The progress has brought more advantageous living conditions. Along with the benefits, the negative events, such as natural disasters and man-made industrial accidents of great extent, have emerged. Fearsome disruptive events arise from scientific and technical progress. The hazards of such an anthropogenic extraordinary events cause deaths and damage of the people, assets and living environment. These inflictions are increased by the development of new sources for meeting a demand and innovations of production technologies capacity. Infrastructure, designed for meeting a demand is mostly endangered by industrial accidents and environmental disasters. Moreover, it can be distinguished among epidemics, pandemics, epiphyte and epizootics. Besides such events, the humankind is also threatened by itself in connection with wars, genocides, international terrorism and organized crime. These phenomena are the major reasons, why assets intended for population needs satisfying are critically vulnerable.

Assets represent everything that any organization or organization perceives as valuable and it can be eliminated by activated threats, i.e. perils. In business terms, it is considered not only a property but also the employers with their abilities and skills. In respect of this fact, it is accepted as “firm assets” or “company assets”. Another

J. Hřebíček et al. (Eds.): ISESS 2013, IFIP AICT 413, pp. 302–310, 2013.

meaning of the term "assets" appears in area of information protection. The "information system assets" can be understood as hardware, software, information system documentation, classified and other critical information that are stored in the information system [1], [14].

2 Needs for Change in the Understanding of Threats

Infrastructure protection is a topical issue nowadays. The risk of various extremist and terrorist actions is very serious in the present time. We believe, this danger is rather underestimated due to the inclusion of Czech Republic into the group with low terrorist attack risk [10]. Despite of above mentioned, terrorist threats became a much discussed subject in professional community. Here, particular areas, technologies or states that could be the next terrorist targets, are controversial and often fuzzy.

To ensure the defence against these attacks on time, various instruments of security, crisis, and emergency management are used. Their basic parts consist from the activities, covered by contingency and emergency planning, which are based on the analysis and assessment of risks and threats. It is an expert analysis of the required goals, which identifies the appropriate ways of goals achievement, and person-oriented leadership that supports the creative work and mutual collaboration [10].

Preventive measures, protecting information infrastructure elements are the most effective but they require the availability of necessary technologies, economic resources and personal qualities. In developed states, instruments for security management are used that help to ensure the high security of communication and information infrastructure elements.

The technology is a key factor in protecting information infrastructure elements [8]. It is not necessary to invent and develop new technologies for the protection and security of individual subjects. It is possible, and for economic reasons often necessary, to use common technologies with a slight modifications or in a new use cases. These procedures create opportunities to secure the selected infrastructure objects at relatively low costs.

There are many research institutes dealing with science and research in information technologies. They toy with the question of the use of common security technologies and other security options that use the principle of COTS (Commercial Off The Shelf) as much as possible. That means the maximal utilization of commercial products and services to create a specific system or technology [13].

3 Security Environment of Information Systems

Each organization should assure security of its information system by reason of property and data loss (or theft) possibility. Comprehensive identification of assets is integral part of the protection securing. The identification consists in compiling a list of organization information system. Other part of the identification process is represented by determination of assets vulnerability within the system realized by application of methods intended for data gathering. The aim of this step is to create the register of assets and system vulnerability (weak points) for the reason that the vulnerability may be the potential target of threats [2].

The active and passive prevention is essential for the assets security. The purpose of active prevention (or just prevention) is to reduce the threat (before its activation as the peril) and potential damage of the assets. It includes:

- Threat elimination or reduction and its transfer,
- Asset resistant strengthening, e.g. building guarding.

The passive prevention (or preparedness) is losses reduction after activated threat. The passive prevention includes:

- Information about threat activation,
- Operations during emergency event occurrence,
- Clearance operations, loss reduction and prevention of domino and synergetic effects.

Principally, building up the preparedness results from the vulnerability determination, because the preparedness can be defined as an ability to manage any emergency event or crisis. On the one hand, the preparedness refers to a community preparedness level. On the other hand, it is linked to the preparedness level of rescue system integration. The preparedness should cover the protection of all assets and it manages all consequences of any emergency/disruptive events. Therefore, it means that any organization has to design such organizational structure of all resources in order to ensure efficient mobilization at the appointed time and place.

Although, the preparedness means creation of certain safety measures because it is impossible to be prepared for every threats. The design of preparedness should contain more than simple balance of resources (staff and equipment), which is more frequent than desirable. The preparedness is mainly aimed at two states within the framework of crisis management – contingency and emergency states.

The organization should make its own security policy that should contain base rules for ensuring the security of its assets with the help of organizational, personal and technological measures. The security policy helps to manage difficulties, connected with intense utilization of information systems that are perceived as essential resources for any organization and its performance [11].

The security policy is based on a security survey, processed by informal team, organized from one external specialist and staff members, responsible for particular areas regarding security. The security survey deals with assessment and description of the security situation within the organization. It consists from the identification of organization assets, the assessment of their importance and the detection of security weaknesses. The planning of basic security measures is also integral part of the security survey. The survey scope is determined by organization management, which should reflect the security as a complex issue. The comprehensive processing also enables efficient access and implementation of security policy.

is recognized as a weakness of certain asset. The weakness can be the target of one or more threats. Therefore, it indicates the possible extent of damage to certain asset.

The security policy objectives are focused on information documentation and information system operations. Following objectives have ensured of interoperable:

- Confidentiality – data leak protection,
- Integrity – asset protection against unauthorized and random modification and guarantee of asset accuracy and completeness,
- Accessibility – stable access to assets in accordance with organization objectives,
- Incontestability – clear identification of transaction author or communicating parts,
- Correspondence between legislation and obligations – the legislative, contractual obligations of the organization.

Benefits of security policy are:

- Uniformity in information management,
- Quick recovery after incident,
- Adoption of efficient measures – future prevention of errors.

4 Asset Evaluation on Security Environments

The value of the information system is recognized as the basic attribute that is derived from objectively quantified price of the system and/or from subjectively evaluated importance of the system by certain organization on certain security environments. One possible option of asset evaluation is to assess potential impacts of undesirable incidents on the organization. Its interests may be directly or indirectly affected by data leak, modification, inaccessibility and/or damage on the asset. Such incidents may consequently result in loss of income or profit, market share, or image and reputation. The organization has to count with all these factors within the framework of asset evaluation.

The information value is often relative in connection with the evaluation process and the evaluator point of view. The typical example of this problem is linked with information which may be perceived as valuable or not, e.g. impact of harmful substances on living organisms, or current economic score of bond issuers. The assessment of the asset value may be based upon the level of impact, measured in money units and associated with the asset damage or loss.

In the asset evaluation, the following aspects have to be taken into account at various security environments:

- Purchase price (or costs),
- Asset importance for organization existence and activities,
- Damage abatement costs,
- Speed of damage control,
- Profit characteristics,
- Others, e.g. potential asset profits.

In the asset evaluation is desirable to divide it into appropriate groups, according to their common features. Assets may be classified as computer assets, security assets, commercial assets and services. It is also necessary to assign owner to each asset. The owner is an individual who is responsible for asset development, production, maintenance, utilization and security. This owner can be viewed as the real holder with all property rights [2, 3].

The determination of the asset value in connection with the impact assessment, which may result from the loss of the asset confidentiality, availability or integrity, it includes selection of scale and evaluative criteria. The scale may be expressed in money units and/or qualitative values. The qualitative values are perceived as numerical or verbal values (from low to critical value). It is practical to use colour resolution and order as you can see in table 1.

Table 1. Example of qualitative evaluation of assets [2]

1	No impact on the organization
2	Insignificant impact
3	Difficulties or financial loss
4	Serious difficulties or financial loss
5	Existential difficulties

The principle of the asset (information system) value determination is based on costs derived from impact of damage to the organization in connection with confidentiality, availability or integrity losses at pertinent security environments. The evaluation may have different results in respect of the viewpoint used during the evaluation. Therefore, the asset may have different values. The final value can be determined by maximal value, by using calculation of average value or using sum of individual values. It is important to use the same method for the evaluation of each asset. The most frequent method is represented by the average calculation. Individual viewpoints are evaluated with the help of the scale illustrated at the table 1. and the final value is calculated. Final asset values are used for risk analysis and calculation of expenses set for the asset protection [12].

The software can be used in the asset evaluation. The organization may choose from specialized software or spread sheets (e.g. LibreOffice or OpenOffice). The organization has to define the scale and evaluative criteria in order to carry out the asset evaluation. This scale may be qualitative or quantitative.

During the asset evaluation, possible threats and impacts on the organization are assessed in respect of the possibility that certain threat will be activated. The threat can potentially trigger undesirable incident, which may result in damage to the system or the organization and its assets. Threats may be natural or anthropogenic and they may be intended or random. The damage may be classified as temporary or permanent.

Many different threats potentially lead to undesirable damage of the assets. It is necessary to identify such threats and assess their likelihood. Therefore, there is enough space for realization of the risk analysis. The term “risk” means a probability that given threat will occurred and cause direct or indirect damage of the organization.

5 Risk Analysis

Risk analysis is defined as a process of likelihood assessing of security failure that may result from threat occurrence, assets vulnerability and accumulated impacts on particular assets. The basic step is to determine adequate security level according of the asset value, which includes cost and risk analysis. The purpose of the analysis is to detect weaknesses of assets and to determine the risk level for each vulnerable asset and threat. Risks have to be reduced to acceptable level. The residual risks arisen from inefficient risk minimization have to be adopted. There are several methods for risk analysis implementation, e.g. informal procedures with the use of individuals' knowledge and experience and/or structured procedures. Risks can be also evaluated with the help of scale with defined points according to risk level or by using your own method or appropriate software. A list of risks is the output from this procedure [2-3].

The risk analysis should lead to selection of appropriate security measures. After the identification and assessment of risks and revision of existing and planned security measures, there are so-called risk residues. Risk residues can be accepted in the case of their low likelihood or if the organization has financial limits in connection with measures availability, or they are not acceptable. If they are not acceptable, the risk analysis has to be performed again, but there is a possibility of adopting such measures which are expensive or useless [2-3].

6 Information System Protection

In ensuring organization security, the key task is protection of the people, information and other properties on relevant security environments. These elements belong to the fundamental assets of the organization. The protection level is influenced by availability of money, people, time and other factors. The protection level is also influenced by organization willingness to accept certain risk level. There are many threats, which endanger the organization information systems. Therefore, it is necessary these threats to identify [5].

Data stored in information systems may be intentionally or unintentionally misused or threaten by a nature. Information system protection is understood as protection from viruses, hackers, spam, irresponsible users and natural disasters.

According of the legal act about information protection [15], the protection of information or communication systems is defined as a system of measures for ensuring confidentiality, integrity and availability of classified information stored in information system. This definition implies that information security consists in many rules and mechanisms for ensuring data confidentiality, integrity and availability. Therefore, information security is extremely complex issue.

Data confidentiality represents prevention of unauthorized access to the system. Data integrity security signifies prevention of unauthorized data modification. Requirement of data availability lies in ensuring access to the system in the right time [6]. Basic components of information system security are illustrated at the Fig. 1.

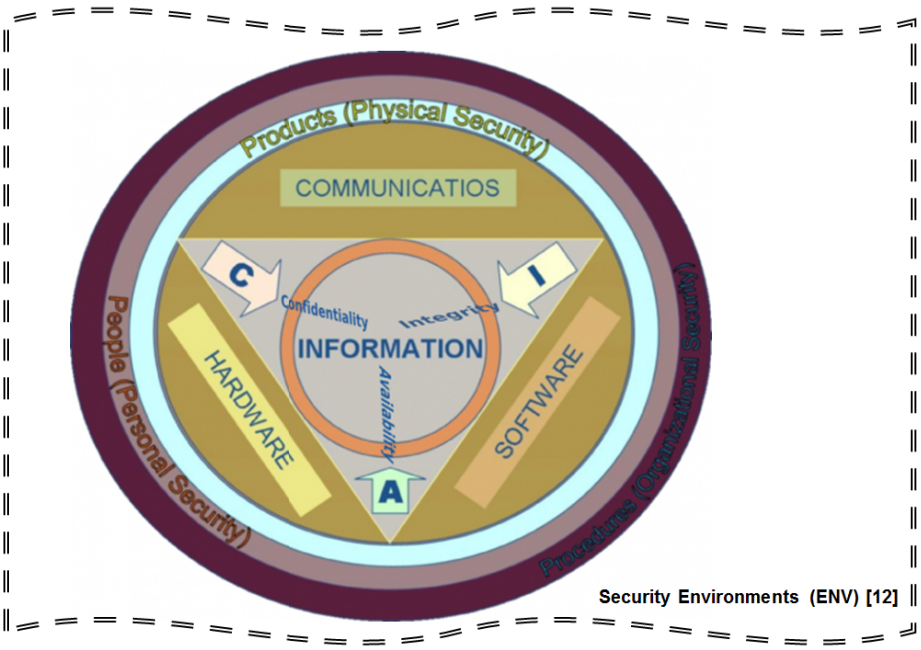

Fig. 1. Information Security Components [4, 12]

In recent years, the progress of ICT has brought certain need for bigger amount of collecting data within information systems and databases. It has resulted in a possibility of information systems destabilization. Today, we can hack into any information system, disturb any military operation, and connect people ideologically all over the world with help of any electronic device [6]. Threats endangering information system security may have fatal consequences, not only as unconstitutional impacts on privacy or personal integrity, but also as violation of national security. Therefore, importance of information system protection reposed on government authorities and private sector is significant [9].

Protection of assets owned by organizations is very important in view of business plans. Entrepreneurs act in more complex legal environment, where they may be exposed to unexpected turns and attacks, which threaten their assets. If their business is spread abroad, then it is necessary to apply foreign law, the situation is even more complicated and risks are higher. Planning the structure aimed at asset protection, that is able to eliminate or reduce adverse impacts when emergency event occurs, is needed [5].

7 Process Approach to Asset Protection

The aim of business process modelling is to create model of processes in order to understand all activities, relations among different activities and all assets and their roles within a process. Every process has several basic characteristics. In asset protection, especially

crisis asset protection, the creation of appropriate set of activities is emphasized in order to preserve process potential even during emergency event occurrence. The continuity process principle focuses on problem mentioned above [12].

Process management focuses on integration of activities within the organization for more rapid and flexible cooperation [7]. It optimizes activities of all processes from the first supplier to the end-customer, and it delegates responsibilities for any process. Performance measurement of individual activities enables easier identification of specific problems. It addresses problem causes. Therefore, it has significant value because in the savings of the money and other resources, which can be, on the contrary, spend for elimination of impacts as consequence of activities disharmony. The process management supports teamwork, brings higher flexibility, enabling better sharing of knowledge and maintains communication during whole process.

8 Conclusion

The majority of the organizations do not focus on information systems protection during times of prosperity. Organizations accumulate certain amount of assets and information, which may be threaten in case of extraordinary event occurrence and they may lose their activities and stable profit. The organizations should make their own security policy that should contain base rules for ensuring the security of its information systems with the help of organizational, personal and technological measures. Therefore, it is important to prevent such events and select appropriate measures in order to protect organization assets.

References

1. Allen, R.: The PENGUIN English Dictionary. Penguin Books (2003)
2. Božek, F., Urban, R.: Management rizika. Univerzita obrany, Brno (2008)
3. Božek, F., Ješonková, L., Dvořák, J., Božek, A.: General Procedure of Risk Management. Ekonomika a management 3, 15–24 (2012)
4. Dardick, G.: Cyber Forensics Assurance. In: The Proceedings of the 8th Australian Digital Forensics Conference, pp. 57–64. Cowan University, Perth Western Australia (2010)
5. Halibozek, E.P., Kovacich, G.L.: Securing corporate assets: Protecting a business against cloak-and-dagger tactics requires a manager's eye for efficiency. Industrial Engineer: IE 35, 39–43 (2003)
6. Knopová, M.: Bezpečnost dat v informačních systémech. Ikaros 15 (2011), http://www.ikaros.cz/node/6946
7. Ludík, T., Navrátil, J., Langerová, A.: Process Oriented Architecture for Emergency Scenarios in the Czech Republic. World Academy of Science, Engineering and Technology 1, 2342–2351 (2011)
8. Ludík, T., Ráček, J.: Process methodology for emergency management. In: Hřebíček, J., Schimak, G., Denzer, R. (eds.) ISESS 2011. IFIP AICT, vol. 359, pp. 302–309. Springer, Heidelberg (2011)
9. Mitnick, K.D., Simon, W.L.: The art of deception: controlling the human element of security. Wiley, Indianapolis (2002)
10. Proházková, D. a kol.: Bezpečnost a krizové řízení. Police history, Praha (2006)

11. Urbánek, J.F., et al.: Scénáře adaptivní kamufláže. Tribun EU, Brno (2012)
12. Urbánek, J.F., et al.: Crisis Scenarios. Univerzity of Defence, Brno (2013)
13. Urbánek, J.F., Průcha, J.: A Development of Wireless Interoper-mobile Application for Outdoor Operation Management. In: 8th Int. Conf. on Electronics, Hardware, Wireless and Optical Communications, EHAC 2009, pp. 57–64. WSEAS Press (2009)
14. Czech Republic Legislation Decree. 523/2005 Coll., on the security of information and communication systems..In Czech Republic Statute Book
15. Czech Republic Act No. 412/2005 Coll., on the protection of Classified Information and Security. In Czech Republic Statute Book