CONDITIONS OF MANAGING THE EFFICIENCY OF THE INFORMATION SYSTEM WITHIN A BUSINESS SYSTEM

Željko Hutinski
Faculty of Information and Organization, Varaždin
e-mail: zhutinsk@foi.hr tel.:042/214-809

Neven Vrček
Faculty of Information and Organization, Varaždin
e-mail: nvrcek@foi.hr

Tedo Vrbanec
Visoka učiteljska škola Čakovec
e-mail: tedo.vrbanec@vus-ck.hr

Abstract

Basic features of the contemporary business systems are massive subsystems and elements, complex relationships, dynamic changes and spatial dislocation of individual parts. To manage such systems, it is necessary to construct adequate information backup. The existence and success of the business system depends upon this backup; hence the emerging need for protection of the information system functionality, as well as for protection of the content upon which the success of the business system depends. The protection can be constructed in several different ways. The paper presents the results of researches of the approaches to the construction of information system security. It also provides the model for construction of the security system that enables management of the security system efficiency. It is based upon the security standard ISO 176799:2000.

Key words: Business system, information system, security, management.

1. Introduction

Functionality of the business systems is increasingly more leaning upon the information backup. Many organizational forms of business systems cannot exist in their present form without information system backup. For this paper, the features of the business systems can be reduced to:

- Massiveness of the organizational units of the business systems
- Complexity of relationships between parts of the system
- Dynamical changes within individual parts of the system, as well as within the system as a whole
- High spatial dislocation of individual parts of the system.

The functionality of a business system with the features of the individual parts listed above can be ensured only by applying information technology. This means monitoring and evidencing state of individual parts of the system, monitoring movements of business and technological processes, grouping of the information needed for every level of business decision making, helping in making the right business decision, communicating with the market, monitoring development etc. All these actions are based upon the data stored in the data bases, algorithms of basic content transformation and network communication, i.e. submitting the desired content to the target group of the users. Such dependence of the business system upon data, information and communication requires adequate level of security for the basic premises of the organizational functioning of the system. There lies the basic reason for the need to construct security system of the information system. Its functionality depends upon the integrity of the information content, upon its precision, upon the constancy of the written content, and upon constant availability. These demands are in contradiction. From the one side, there is the demand for the availability of the content, which is often realized through the use of public communication services; from the other side, there is demand for protection of the integrity and protection from non-authorized use or change of the same content.

Therefore, a security system should be constructed which will fulfill all these demands, and which, at the same time, will not present an obstacle for the application in these conditions.

2. Information system security

To be able to approach the construction of the security system, we must define the notion *information security*. Information should be treated as an asset, which like all other business assets has certain value for a business system, and therefore requires adequate protection and security. Information security protects the data and information from wide range of threats, as to ensure the continuity of the business, to reduce the business damage to the lowest possible level, and to increase the level of return of the investment – business profitability.

Information exists in many forms. It could be written or printed on the paper, and in this case it would be written on the analogue material media (paper), but it also could be written in the digital form – electronically stored. It could be submitted by the classic mailing system or by e-mail, it could be showed in the films or told in conversation. Whichever form it has, whichever media is used to communicate it or to store it, it should be properly protected.

To be able to manage individual and common interest of greater number of various business subjects, one should construct the information system according to some common criteria. The common principles and methodological approach should also be used in construction of the security system. The common and unified approach to the security of an information system can be achieved by application of a common norm which unifies the procedures of security system introduction and ensures equal criteria for choice of the risk reduction measures. There are many national norms that have such characteristics, like BSI, DIN, AFNOR and others. Also, there are very rigorous norm of the institutions such as NASA, DoD etc.

Within the frame of Joint Technical Committee with IEC JTC 1, ISO organization has the subcommittee 27, dedicated to the designing of the information system security norms. Until now, 33 such norms have been designed. The following table gives a review of 4 randomly selected norms.

Table 1: Review of some ISO norms from the field of information system security

No.	Norm	Field of application
1.	ISO/IEC 9796-3:2000	Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms
2.	ISO/IEC 9798-2:1999	Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms
3.	ISO/IEC TR 13335-2:1997	Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security
4.	ISO/IEC 17799:2000	Information technology – Code of practice for information security management

Source: (Krakar, Hutinski, Rotim.Tomić)

Besides these 33 norms which are mostly used in European business areas, a variety of norms also exists designed for application in other geographical locations and areas. Simple Internet search with the use of key words "Information security" yields a review of 78 such norms in the field of information system security.

Besides so-called technical norms, intended for the information system security, there also exist a visible tendency toward establishing integral systems of information security management. In 1995 British Standard Institute has published two such norms, whose goal was to establish integral systems of information security management. These norms were:

- BS 7799-1:1995 Information security management – Part 1. Code of practice for information security management systems and
- BS 7799-2:1995 Information security management – Part 2. Specification for information security management systems.

It is interesting to note that, within the frame of the mentioned ISO/IEC JTC 1/SC 27 IT Security techniques, the development of the norms for information system security was organized in such way that 3 work groups were formed: WG 1 Requirements, security services and guidelines (conducted by English BSI), WG 2 Security techniques and mechanisms (conducted by Belgian IBN) i WG 2 Security evaluation criteria (conducted by Swedish SIS).

As a result of these efforts, especially work of the WG 1, in 1999 new versions of these norms were created. First of these norms (BS 7799-1:1999) was accepted by ISO and IEC as the norm ISO/IEC 17799:2000; also, the second norm will be published soon.

The norm ISO/IEC 17799:2000 has the following 10 chapters (without introduction)

- Security policy
- Organizational security
- Classification and control of the assets
- Personnel security
- Physical and environmental security
- Communication and operative management
- Surveillance of the approach
- Development and maintenance of the system
- Business activity continuity management
- Complaints

By application of the norms, notably the norm ISO 17799:2000, all preconditions are fulfilled for our practice to approach the designing and implementation of the integral systems for security management in the information systems.

2. Steps in the establishing of the security system

The steps for realization of the security system can be cited in detail, or more globally. In the basic level of application, the following steps should be noted:

1. Definition and application of the security policy
2. Security risk assessment
   a. Assessment of the importance of the data content
   b. Information assets inventory
      i. Factors outside of the business system (Legal acts and norms, bills, traditional law)
      ii. Factors within the business system (Statute and regulations of individual business systems and
   c. management assessment of the importance of a separate content for functionality of the business
   d. system)
   e. Identification of threats to the separate content
3. Choice of measures for risk reduction
4. Monitoring the efficiency of the system

2.1. Defining and introduction of the security policy

The highest management level of the business system should clearly express the policy and the goals of the business system, as well as the support for and dedication to

the information security, by introducing and applying the information security policy in the whole organization. The security policy document should be approved by the management, and it should be introduced to all employees. The orientation of the management should be clearly expressed; also, the organizational approach to the information security management should be defined (ISO 17799:2000).

It is necessary to define security demands within the business system. There are three main sources of such demands. **First source** is the assessment of the risks which the organization faces. The risk assessment is used for identification of threats to the assets, identification of vulnerability to these threats, and the probability for their appearance; also, it is used for assessment of potential consequences.

Second source are legal, statutory and contract obligations which should be fulfilled by the organization, its partners, subcontractors and service providers. **Third source** is the group of principles, goals and requirements for data processing, developed by the organization as the support for its activities.

2.2. Security risk assessment

Security requirements are identified through methodical security risk assessment. The amount of resources intended for the control mechanisms should be balanced with the predicted business damage which results from the security failures. Risk assessment techniques could be applied to the whole organization, to certain parts of the organization, and also to individual information systems, individual system components or services, and the solution should be practical, realistic and useful.

To make a valid risk assessment, the following should be done:

1. Assessment of the importance of the data content, which consists of:
   a. Making inventory of the information assets
   b. Determining the factors outside of the business system (Legal acts and norms, bills, traditional law)
   c. Determining the factors within the business system (Statute and regulations of individual business systems and management assessment of the importance of a separate content for functionality of the business system)
2. Identification of threats to the separate content

After making of these two documents, the risk assessment can be approached through the choice of the adequate methodological actions. The methods that are most often used are quantitative and qualitative; the choice of the method depends upon the maturity of the information system, i.e. knowledge of the forms and frequency of the threats, as well as the amount of damage they have done.

The risk assessment is a systematic consideration of the business damage as well as the realistic probability for security disturbances. Business damage may be the result of the security disturbances, related to the potential consequences of the loss of confidentiality, integrity or accessibility of the information or the asset. The probability for such disturbances are considered in the context of dominant threats and vulnerability, as well as presently implemented control mechanisms.

The results of such assessment will provide help in determining and implementing the adequate management actions and priorities for managing the information security, and also in implementing the chosen control mechanisms for protection from the security risks. The process of risk assessment and the choice of control mechanisms may be conducted several times, because various parts of the organization or information systems need to be covered.

The assessments of the security risks should be conducted at different levels, depending upon the results of previous assessment and the change in the levels of risk which the management is prepared to take. The risk assessment is often made at the highest levels, to determine priority for individual resources in the areas of high risk; after that, it is focused to the more detailed levels, to make insight in the specific risks.

2.3. The choice of risk reduction measures

Once the security requirements are identified, the control mechanisms should be chosen and implemented, so the risks can be reduced to the acceptable level. The control mechanisms can be chosen from the norm ISO 17799:2000, or from any other source of the control mechanisms; also, new mechanisms can be constructed with the purpose of satisfying the specific needs.

There are many different ways for risk management; we will show here the examples of more general approaches. However, it should be noted that some control mechanisms are not applicable in all information systems and environments, and may not be practical for every organization. The basic interest of security measures are data. Data are an abstract category, so we must materialize them on some of the material media (analogue, digital or both)

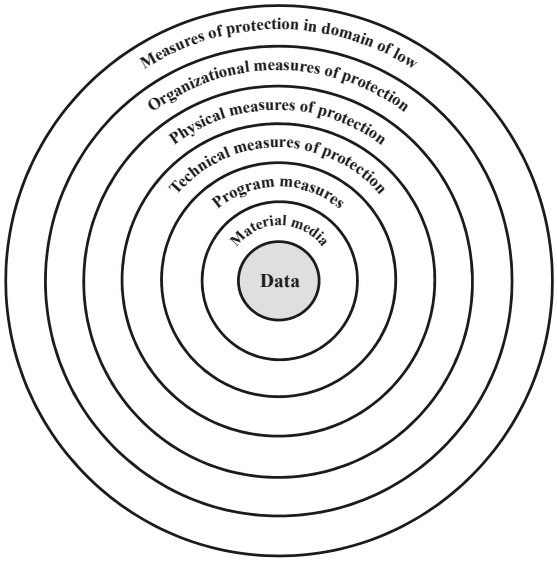

Figure 1. Measures of protection of the information system

When computers are used, then the following program protection measures can be applied:

- Measures of protection at the level of operational system
- Measures of protection at the level users' program backup
- Measures of protection at the level of data base management system
- Measures of protection in the network transmission (cryptosystems)
- Safety content duplication (backup)
- Measures of protection against viruses

Measures of protection which will be used in a specific situation depend upon the choice and upon their combination with the goal to achieve certain level of security in relation to the amount of resources which will be invested.

2.4. Implementation and monitoring the efficiency of the implemented security system

The experience has shown that, for successful implementation of the information security within the organization, following factors are often pivotal:

- Security policy, goals and activities that reflect business goals
- An approach to the information security implementation that is consistent with the culture of the organization.
- Visible support and dedication of the management
- Good understanding of security requirements, risk assessment and risk management
- Acceptance of the guidelines of the security system from all levels of management and employees
- Distribution of the instructions about information security policy to all employees and contract partners
- Provision of adequate education and training
- Comprehensive and balanced system of measures for evaluation of the effects in management of the information security, and also system of measures for gathering feedback with the goal of improvement

The question of the security system is extremely important for systems of state administrations, because of protection of the privacy of data which they have and use every day. Therefore, in the process of designing information system for this project documentation, all mentioned factors of security system should be considered.

Monitoring and evidencing the security accidents, regardless of the way in which they have manifested, is the foundation for identification of weak measures within the protection system. Based upon evidence of accidents in the information system, an assessment of security failures can be made; in this way, the system can be upgraded, so the security practice is matched with the required level of security, defined by the protection policy.

3. Management of information system security

To manage the information system security means, like the other forms of management, to constantly guide the system toward the goal function. If, during the construction of the security system, we have defined goal function, i.e. path of development and level of security of an information system, the other actions should be focused upon prescription of the measures through which the desired security level can be realized.

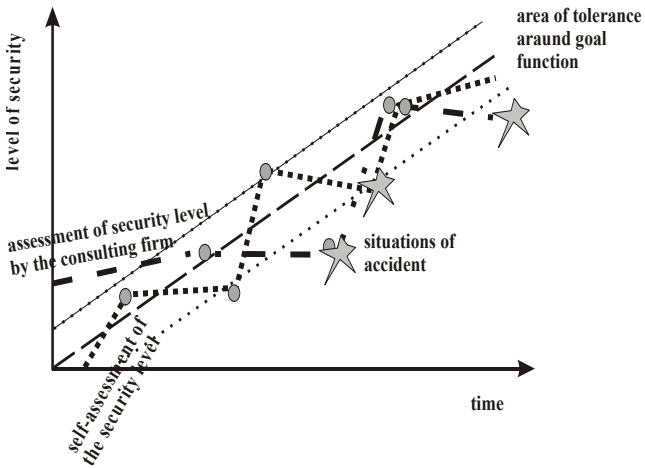

Figure 2. Bringing the security toward the goal function based upon the assessment of outside and inside evaluators

If we want to reach a satisfactory security level, we should know in any given moment how the system will act in relation to implemented measures. This knowledge can be based upon our own assessment of the security level. Such assessment is always subjective, and presupposes the security measures which were not described here. The change of work places of the employees decreases the system of security measures because of lack of organizational instructions which could be understood and applied in the unified manner. The second level of knowledge about the functionality of the measures may come from a neutral consulting firm which can simulate situation of accident and assess the efficiency of the measures. The most undesirable form of knowledge about the efficiency of the measures is the real accident. If this happens, the cause of accident should be found, and the measures should be modified as to decrease the level of threats – this is security system management.

There are several techniques of information system security management through accident management. One of those is Tripod – Delta. It was developed at the University of Leiden and Manchester for the needs of Shell. It can be applied if three basic preconditions are fulfilled:

1. Coherent security policy which sets realistic security goals.
2. Developed security culture, so the measures can be realized.
3. Developed measures for assessment of the efficiency of the security measures (General Failure Types GFT)

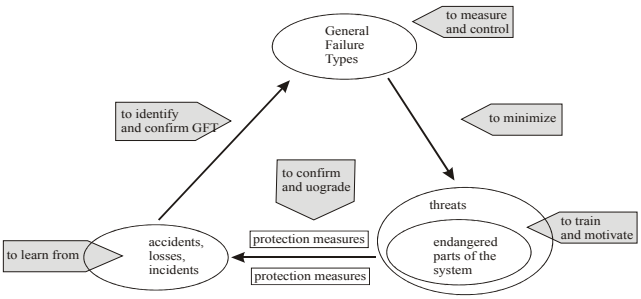

Figure 3. Structure of Tripod – Delta method of assessment of the impact of threats to the information system (Reason, 133.)

The frequency of threats to the information system was measured by application of the described method. The research was conducted by applying 20 instruments per threat. When irrelevant threats are removed, the results are the following frequencies of different groups of threats, as shown on the figure 4:

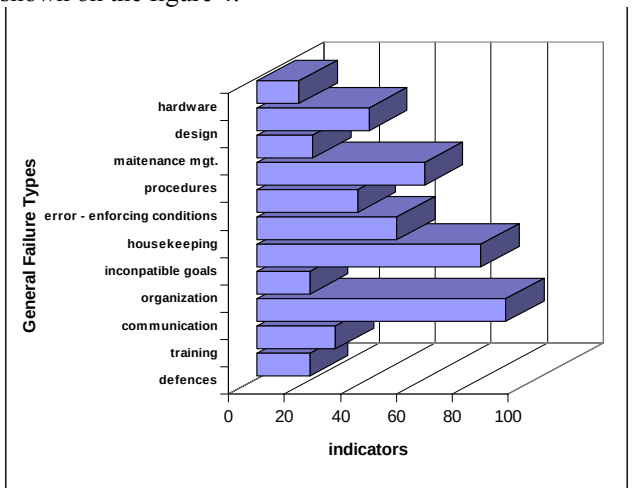

Figure 4. Frequency of threats by form of threat

This research should be conducted for every separate setting, so the frequency of various forms of threats to the information systems can be found. Every setting has different evaluation of the data content value, different threats to this content, and different measures for decreasing the level of threats. Such survey of threats and their frequency is base for risk assessment, and for the changes in measures of protection that influence the security system.

4. Conclusion

Business systems are dependent on information, so they require certain level of information security. Since it is necessary to exchange the contents with large number of business subjects, the systems of content protection of other business systems should also be taken into consideration. To achieve unified and balanced approach in the implementation of the security measures, unified methodological preconditions for construction of security systems should be used. These measures are defined through the norm ISO 17799:2000, which prescribes methodological approach and areas in which protection measures need to be applied. The application of the norm in the construction of the system ascertains the unification of the approaches and the similarity of security levels for separate group of content.

Once implemented, the security measures cannot provide the same level of protection during the longer period of time. The importance of the protected content changes, therefore the level of risk also changes. The change of the level of risk results in the change of measures implemented to achieve the desired level of security. To monitor the changes in the business system and to respond by making changes in security measures means to manage the security system. The knowledge about the need for change of the measures can be gained through systematic risk assessment, or through evidence of the situations of accident which point to the security failures. For such approach to the changes, every accident needs to be evidenced and studied; if necessary, intervention should be made in the system of security measures.

In Croatia, there is not yet enough consciousness about the need for systematic construction of protection of the information systems. Different settings react differently to the need for implementation of the security measures. In many settings, partial measures are being used, but they are rarely described and documented, so it is hard to talk about security system management in such conditions. The research has been made on business systems in various sectors of activity. The results are shown on the Figure 5.

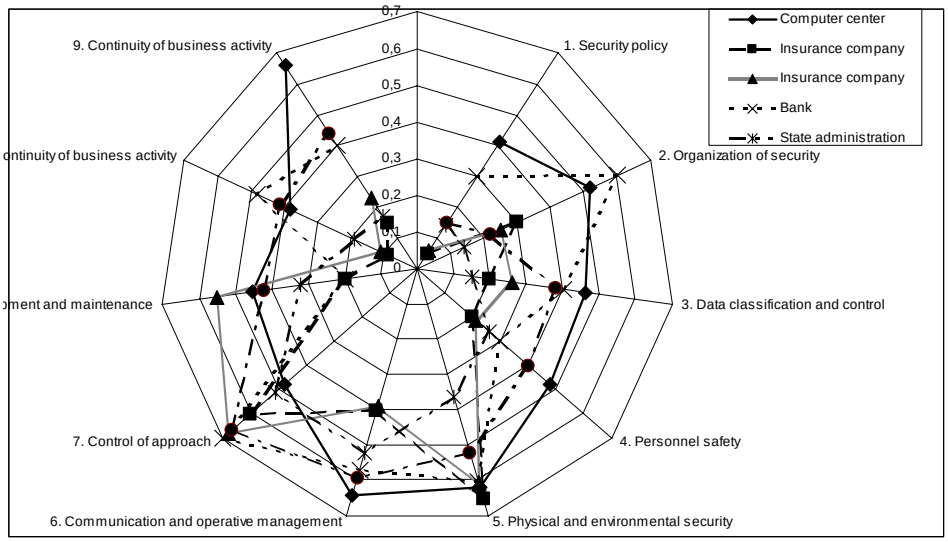

Figure 5. The degree in which six business systems in Croatia are matched with the norm ISO 17799:2000

It is obvious from this figure that the banks and the computer centers also have relatively low accordance with the norm. Partial measures are present, but they are not described and documented in adequate manner, so the direction of security system functionality cannot be followed. Therefore, there is no possibility for system management, and also no possibility to upgrade the system to the satisfying level of risk. In such conditions, there is also no possibility for certification of the security system, and the measures cannot be compared and accepted at the international level.

Literature:

1. Adams, C., S. Lloyd, (1999.), Understanding Public-Key Infrastructure: Concepts, Standards and Deployment Considerations, Macmillan Technical Publishing, Indianapolis
2. Apter, D., E., (1971.), The Politics of Modernization, Chicago, University of Chocago Press.
3. Black, C., E., (1966.), The Dynamich of Modernization, New York, Harper & Row.
4. Bubaš, G., Kliček, B, Hutinski, Ž. (2001.) Decision tree analysis of the predictors of Internet affinity. *12th* International Conference on Information and Intelligent Systems, Varaždin, Croatia.
5. Deise, M., Nowikow, C., King, P., Wright, A. (2000). Executive's Guide to E-Business: From Tactics to Strategy, John Wiley and Sons, Inc., New York.
6. Diffie W., M. E. Hellman, (1979.), Privacy and Authentication: An Introduction to Cryptography, Proceedings of the IEEE, vol. 67, n. 3, p. 397-427.
7. Grupa autora, (2000.), Digital Economy, Economic and statistics Administartion, Office and Policy Development, Scretariat on Electronic Commerce U.S. Department of Commerce, Washington, DC 20230,
8. Hutinski Ž., K. Kero, m. Žugaj, (2001.), Correlation of Informatic Education in Realization of Dinamic and Distributed Systems, 20. Posvetovanje organizatorjev dela, Management in globalizacija, Portorož. 28.-30. Marec 2001., Zbornik posvetovanja z mednarodno udeležbo, Univerza v Mariboru, Fakulteta za organizacijske vede, str. 79. – 87.
9. Krakar Z., Ž. Hutinski, S. Tomić-Rotim, (2001.), Sustavi upravljanja sigurnošću u informatici - korak koji slijedi, Zbornik radova, Treća hrvatska konferencija o kvaliteti, Cavtat, 25. do 27. travnja 2001., str. 63. - 69.
10. Levy, M., J., (1966.), Modernization and the Structure of Societies, Princeton, Princenton University Press.
11. Reason, J., (1997.), Managing the risk of organizational accidents, Asgate Publishing Limited, Hampshire, England
12. Scheiner B., (1996.) Applied Cryptography, 2nd Edn., John Wiley & Sons, New York, 1996.
13. Vrček, N., Kermek, D., Brumec J., (2001.), Metode i alati za projektiranje informacijskih sustava, Sustavi za planiranje resursa poduzeća i elektroničko poslovanje, CASE 13, Opatija

1. Pravilnik o tehničkim pravilima i uvjetima povezivanja sustava certificiranja elektroničkih potpisa, Narodne Novine, Jul. 25th 2002, http://www.nn.hr/clanci/sluzbeno/2002/1472.htm, accessed Feb. 17th 2003.
2. Strategija razvitka Republike Hrvatske, Hrvatska u 21. stoljeću, Informacijska i komunikacijska tehnologija.
3. Zakon o elektroničkom potpisu, Narodne Novine, Jan. 30th 2002,
4. ISO/IEC 9796-3:2000, Information technology
5. ISO/IEC 9796-3:2000, Security techniques
6. ISO/IEC 9796-3:2000, Digital signature schemes giving message recovery
7. ISO/IEC 9796-3:2000, Part 3: Discrete logarithm based mechanisms
8. ISO/IEC 9798-2:1999, Information technology
9. ISO/IEC 9798-2:1999, Security techniques
10. ISO/IEC 9798-2:1999, Entity authentication
11. ISO/IEC 9798-2:1999, Part 2: Mechanisms using symmetric encipherment algorithms
12. ISO/IEC TR 13335-2:1997, Information technology
13. ISO/IEC TR 13335-2:1997, Guidelines for the management of IT Security
14. ISO/IEC TR 13335-2:1997, Part 2: Managing and planning IT Security
15. ISO/IEC 17799:2000, Information technology, Code of practice for information security management

1. http://www.hrvatska21/,
2. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf
3. http://www.ecommerce.gov