UDC 007:004.056:006
DOI: 10.7562/SE2014.4.01.03
Original article
www.safety.ni.ac.rs

JOŽE ŠREKL[1]
ANDREJKA PODBREGAR[2]

[1]University of Ljubljana,
Faculty of Chemistry and Chemical Technology
[1]University of Ljubljana,
Faculty of Chemistry and Chemical Technology

[1]joze.srekl@fkkt.uni-lj.si
[2] andrejamedvesek@yahoo.com

ENHANCING SAFETY INFORMATION SYSTEMS WITH THE USE ISO/IEC 27000

Abstract: *A company should pay much attention to information systems security. It is necessary to secure the support system of the organization if we want continuity and effectiveness of business. In addition to providing security through technological precautions to prevent intrusion and abuse, it is necessary to pay more attention to the vulnerability and threats caused by the engaged users. Here we refer to unintentional threats, as a result of faulty workmanship or lack of knowledge of the information system. It is important to strive to reduce the possibility of causing the occurrence of incidents which are the result of improper use of information technology, which is due to ignorance. An organization shall consider and identify vulnerabilities of the system and threats to it. We confront the growing amounts of information in electronic form. Ensuring security of information systems (IS) in the workplace involves many steps that a company must adopt and carry out. The vulnerability of the systems is being examined, whereas the form of the new age of terrorism, cyber-terrorism, is being presented. This paper deals with ways of reducing risks and increasing safety and security of IS. It presents possible ways of ensuring the safe use of IS.*

Key words: Information system, management, safety, security.

INTRODUCTION

The work of every person in the economy and non-economy is more and more focused into overall accessibility and interconnection of pieces of information in this information age. Information systems are due to continuous progression part of business systems and the base of each organizational structure, fundamental support component, without which modern societies cannot achieve the set goals. Information Systems Management is associated with the permanent risk of intrusions in IS, damage or theft of information or even the destruction of entire IT systems. The moment of connection to the internet connects us with the dark traps. [1] At the proper management of information, systems in conjunction with an appropriate risk management can achieve a low level of risk, which means the minimum probability of intrusion into the system and the minimum possible consequences of this intrusion. The safety and security of the information system is the aim of any business. To ensure the security of information systems (IS) in the workplace involves many steps that a company must adopt and carry out. The support system of the organization is necessary to secure for continuity and performance. In addition, to provide security through technological steps to prevent intrusion and abuse, it is necessary to pay more attention to the vulnerabilities and threats caused by employees of users.

Information system security is the ability of an information system that under certain conditions satisfactory performs the required functions without unwanted consequences. The information system is the basis of every organizational structure in the current digital age.

Today, the important strategic resources of each organization are knowledge, intellectual capital and information resources. Information security means protecting information against unauthorized disclosure, transfer, modification or destruction, regardless of whether an event is random or intentional. The introduction of information security in accordance with ISO/IEC 27001:2013 provides a comprehensive approach to information security. In accordance with the standard company security policy, other precautions and further procedures and rules, that employees should follow, are formed. [5]

Security in larger organizations is ensured by a systematic approach. As the threats to the security confidentiality, availability and integrity of the property of the information system are increasing, the introduction SISM (System for Information Security Management) is required in organizations. The pretentiousness of introducing the project of the SISM in the company depends on the size, structure, needs, objectives and safety requirements of the company. The system provides greater security to the company, which is associated with well-defined security policy and knowledge of policies on the use of information systems.

The company must take appropriate steps to protect its information system to ensure smooth operation and to prevent damage that would arise from the loss or misuse of information. In order to introduce adequate protection and security it must be aware of the threat

and the potential harm to the system. We often talk about the vulnerability of IS faced by the company. That is why the most important objective of the establishment of preventive steps is to protect against the threats to information systems and actions that may threaten vulnerable information system. Following the risk assessment, the company may also pay measures for reducing risks and increasing safety and security of IS. It is important to determine what are the methods and tools for individual organizations to protect against intrusion by unauthorized users and consequential loss or misuse of data.

INFORMATION SYSTEM

The Vulnerability of IS

The vulnerability of information system is any shortcoming of the information system, which a certain threat can misuse. It is the result of poor information system security against the threat or an activity of an attacker. The vulnerability itself does not cause harm; it is merely a state or series of states, which allows influence of the information system. Threats can take advantage of the vulnerability of the system and cause damage to the IS. [3] Vulnerabilities of different IS may vary; they can be affected by their environment and by the way of use. There are [3]:

- Physical vulnerability, the ISs are exposed to physical interference or attack on the whole system or its individual parts, such as theft, damage, etc.
- Vulnerability because of natural disasters; natural disasters (fire, earthquake, flood, etc.) are unpredictable events that may cause failure, malfunction or limited operation of IS.
- Vulnerability of hardware and software; the development, new technology, lack of time for testing, manufacturing defects result in poor protection and the possibility of intrusion into the system.
- Vulnerability of media for storing information; different media are exposed to various risks that may cause data loss or disclosure.
- Vulnerability of electromagnetic radiation; electronic equipment and components emit electrical signals or they cause electromagnetic radiation (hereinafter EMS), in space that can transmit sensitive information, such as confidential information, trade secrets, personal data, etc. Information which is spread in space in the form of EMS, is possible to be intercepted.
- Vulnerability of electronic communication; email, conversations over internet protocol (VOIP - voice over IP) and rapid forms of textual communication allow the interception and eavesdropping.
- Human vulnerability involves vulnerability caused by the user or administrator of IS or a person. Researches of the majority of attacks and abuses showed that a person is the main for the success of an attack, since the attacker generally does not need to exploit the vulnerabilities of technologies.

Treats to IS

A treat to a company's information system represents everything that can, intentionally or unintentionally, abuse of the vulnerability of IS and cause damage. There are several ways of distribution of threats. Threats can be divided into two groups [3]:

- Threats, which are the result of the geographical scope of the activity of a company and the used technologies and
- Threats, which are the source of human activity and the way of use of IS.

Successful mastery of threats at natural disasters presents a great challenge for professional service. This part of the threat is the biggest unknown for the preparation of possible steps and solutions to reduce threats. Natural disasters are unpredictable, so the magnitude cannot be predicted. A company can organize its operations in accordance with the recommendations of various professional institutes or agencies that deal with natural disasters, but the results of the measures taken for the success or failure can usually only be proved at an unpredictable event. It is therefore important that the company includes a threat assessment plan in case of an emergency (if it has any) and steps that will be implemented in connection with the IS in emergency. To decide whether a company will establish an alternative location in another city or even in another country (e.g. outside the seismic zone) and what steps will be taken to reduce these types of threats are the responsibility of the owner or manager. We can expect easier and faster control action in relation to technological threats. All the companies that use modern technological devices are now facing these treats. With appropriate planning and use of appropriate security technologies such threats are under control. These threats are not dependent on the method of work of employees and the use of IS. [3]

Human threats to the IS in the company are more frequent than the threat of natural disasters. They are divided into external and internal. The involvement of IT professionals, employees and management to successful defend against these threats require. The external threats are associated with intentional threat of attacks on the IS. The purpose of these attacks is to gain unauthorized access or control over information or simply to cause damage to the company resulting from the reduction in performance or inability to complete the operation of IS. These threats can be physical (unauthorized physical intervention) or virtual (e.g. malicious code, fishing, etc.). External threats are carried out by competitive companies, criminal groups, individuals - hackers, government organizations, terrorist organizations and others. Internal threats are intentional and unintentional; they execute within the company. They are performed by employees or contractors who have physical access to the IS or execute unauthorized access to information resources companies. In this set includes threats of data theft or intellectual property rights of companies, misuse of

administrator - access rights, different forms of sabotage and the like. Unintentional internal threats represent users of IS enterprises (in most cases employees). These cases include a security threat due to negligence, ignorance, thoughtlessness or a mere curiosity user of the IS, which can lead to internal incidents or permit the performance of intentional internal or external threats or unauthorized access to the IS business. To reduce the risk in this area the vital awareness of users and clearly defined use of IS and technology is important. [3]

Types of treats

We can classify threats as to the ways of compromising the IS:

Different forms of specific attacks, among which viruses Trojan horses, spyware and various application software that can be attributed to three characteristics: self-reproduction, population growth and free-riding may be included, represent a malicious program. [1]

Intentional abuses by the employees represent a form of threats that are difficult to be controlled. They particularly outstanding in poor economic conditions and high unemployment rate, which is present in today. Employees may exploit their status position in the company due to different personal interests, such as revenge, proceeds, etc. Abuses are divided into three groups [3]: IT sabotage intellectual property theft and deception. This leads to loss of confidential information and intellectual property, reduce data integrity, disclosure of personal / private information, damage to or destruction of key IS, unavailability of communications and the inability of implementing sales activities.

Incautious and poorly educated employees cause careless handling of passwords, opening of unexpected attachments in e-mail, ignoring the dangers of wireless networks and mobile devices, naive answers to a seemingly trivial issues (social engineering), loss or theft of laptops (poor preservation), the reduction of the attention in the implementation of physical security in the workplace and protection of the company's assets. Failure to comply and failure to implement security policy is the result of inappropriate management.

The purpose and goal of the research

The purpose of this work is to fully present the scope of information security; and with the method of theoretical research, which includes the collection and review of existing literature, articles and skills to present the threat of information system vulnerabilities of information systems and measures for the protection of IS. We would like to find the meaning and the influence of the series of standards ISO / IEC 27000 on the safe management of IS.

Searching of the preventive steps to protect against threats to information systems focus primarily on finding steps of good governance with IS to reduce vulnerabilities and threats to information systems, thereby decreasing the potential damage. You could call management information system with minimal risk or short management (management) risks in information systems.

The method of surveying all users of certified standards series ISO/IEC 27000 and randomly selected users without IT certificate will try to determine the differences in quality management and IT security. We assert that it IS safer considering the series of standards ISO/IEC 27000.

METHODS

This method is analytical and experimental. We will analyse the well-known experience described in various sources, based on the facts described in various articles and we created a synthetic argument about the role and the importance of risk management in the information system. The survey was used to test the differences in the risk management system in the field of IS and confirmed the hypothesis about the positive effects of implementation ISMS (information security management system) the level of safety of the system.

RESULTS

Steps to IT security

Setting up the system is interference in a company that has organizational and financial implications. The senior management support is needed to establish a system. No project or initiative can succeed without financial sources and engagement of the employees, which requires the involvement of the top management. At the same time the consent or at least understanding of the majority of the members of the management teams required. We can gain support, understanding and consent primarily by demonstrating benefits for both the organization and the staff of the organization (achieving compliance with all the established safety requirements, improve market position, reduce costs, optimize business processes).

The establishment of a system must aim to achieve the level of information security, which can be determined in clear, understandable and measurable units. These units must reflect the amount of benefits for the company and for the employees. Implementation of information security requires:

- Time for implementation of the project, information security,
- Integration of a number of staff from the organization
- A number of changes in working procedures, responsibilities and technologies,
- Otherwise, dispose of human resources.

Appropriate frameworks for the implementation are the standard ISO/IEC 27001: 2013 and its family members. ISO/IEC 27001 is the leading international standard for

information security management. It is not a technical standard, so it does not describe technical details of MSSI (management system for safety information). It does not focus only on information technology but also on other important goods in the organization, such as personnel, facilities, documentation and exchange of information. It also focuses on all business processes and business amenities. It defines the business rules that reduce the risk in information flow [5].

The standard gives:

- Best framework for compliance with the laws of information safety,
- Better appearance of organization because of the obtained certificate,
- Lower costs avoided due to safety incidents,
- Optimized operating procedures of the organization.

As already mentioned, the standard is designed for developing systematic management of IS, which manages the risks that arise in the process of functioning of the system. Similar to the introduction of quality control under ISO 9001, the use of ISO/IEC 27000 also has to be carried out in several steps:

Planning MSSI:

- Policy and goals
- Risk Assessment & Risk Management
- Report on risk assessment
- Declaration of Conformity performance

Implementation MSSI:

- 4 mandatory procedure
- Risk Management Plan
- Implementation of controls
- Implementation of training, awareness-raising

Checking MSSI:

- Implementation of control methods and review
- Measuring the effectiveness of controls
- Internal verification
- Management review

Improving MSSI:

- Corrective actions
- Preventive activities

Training and building a culture of safety usually require new skills (to design a program for the entire organization, implement the program in parallel with the implementation, and implement the program as a continuous business process). Continuous monitoring of the activities, measurement, testing, inspection and improvement is performed. [7]

Results of the survey

As to these two institutions, 46 companies in Slovenia currently certified standard ISO/IEC 27001: 2005. The survey covered 31 companies, representing 67% of the total. Four-fifths of firms associated the quality of governance (the ISO 9001 certificate) with IT security. Introducing the certificate we can divide the companies into two groups: micro and small enterprises (up to 50 employees) and medium and large enterprises (50 or more employees). The relationship between the size and the price is not linear ($R^2 = 0.2283$).

Table 1. *Average costs as to the following categories of companies [source: own]*

Enterprise Category	Average cost of implementation (€)
1 (micro)	18000,00
2 (small)	18333,33
3 (medium)	28888,89
4 (large)	34285,71

Since the establishment of information security management system is an extensive process, most companies require a year or longer to set up this system. Of course, most likely the length of time of setting up a system is influenced by certain factors such as the size of the company, the manner of execution of the project (external consultants or without one), complexity, activities, etc. The time of setting up in large companies is longer, due to internal procedures and greater coordination.

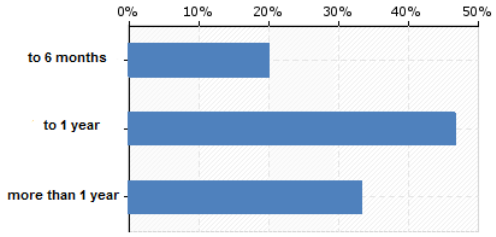

Figure 1. *Time of setting up MSSI [source: survey]*

The result of the analysis of the questionnaire confirmed the expectations that companies with the implementation of ISO/IEC 27001: 2005 reduce the number of incidents. Two thirds of the examinees (63%) link the introduction of MSSI to reducing of the incidents in IS. 77% of the respondents is confident that with the introduction of MSSI they reduced the risk of incidents in the IS. It is associated with the periodic implementation of the risk assessment.

When asking the companies that do not have MSSI we can conclude that they provide security systems with conventional systems of protection (firewall, antivirus, document protection of trade secrets). They believe that they have the information security policy. It was discovered that most of them do not inform their employees about threats for IS, they do not encrypt personal data in the e-mail.

CONCLUSION

The problem of information safety is slowly gaining interest in the management of the organization. This awareness is particularly important because information safety is a managerial activity that in addition to financial resources also provides knowledge management, the right people and proper management policy. The relevant standards help systematic regulating this field. In some areas, more efforts need to achieve full compliance with the standard. This is particularly true for the recording, valuation of assets, the establishment, and regular checking of documents. Strict safety regulations are not always the solution, because the tighter security steps the security is larger, but the working process can be more difficult at such a tightening. A limit among the regulations, common sense and technological solutions is necessary.

Considering all of this, it is necessary to be aware that there is no absolute safety and it is necessary to constantly check the introducing and the results of the introduced control. Usually a relatively expensive project does not have direct visual effects, so projects do not receive much attention. Exceptions are those organizations that have to certify themselves so that they are able to perform their activity.

Obtaining a certificate of compliance with the standard is usually not cheap. It should be noted the cost of external consultants, the cost auditor and the audit, as well as spending time of the employees who should be involved in all phases of the project. Depending on the size of the organization and the maturity of processes such projects can last for a year or more, which of course eventually applied quite a man / months, put in by the colleagues. An organization that obtains a certificate of compliance with one of the family of ISO/IEC 27000 shows the outside world to carry out their activities in a manner that ensures the security of data and information provided by stores and processes. The reference of reasonableness and economic merits of introducing family certificate ISO / EIC 27000 is the introduction of ISO 9001 quality certificate, which also demonstrated economic results.

List of symbols

BS - British Standard

IEC - International Electro technical Commission

IS - Information systems

ISO - International Organization of Standardization

IT - Information technology

MSSI - management system for safety information

REFERENCES

[1] Dimic, M., Kriminaliteta v informacijski družbi, Uporabna informatika, 17, 2009(2), 101-105.

[2] Erznožnik T., Varnost informacijskih sistemov in računalniške zlorabe (Information systems security and computer abuses): Delo diplomskega seminarja, Univerza v Mariboru: Maribor 2012.

[3] Hribar J.: Varna raba informacijskih sistemov na delovnih mestih, Magistrsko delo, Univerza v Mariboru: Ljubljana, 2011.

[4] Hvala D., »Nepotrebna standardizacija«?, Monitor PRO, december 2011, pridobljeno dne: 3.4.2014, dostopno na: http://www.monitorpro.si/111479/praksa/nepotrebna-standardizacija/

[5] Jerman Blažič, A.; Novosti, ki jih prinašajo novi standardi SIST ISO/IEC 27001, 27002 in 27003 ter njihova uporaba v praksi, SIST seminar, Ljubljana, 28.marec 2014

[6] Koščak, D., Varovanje informacij v skladu s standardom ISO/IEC 27000, Diplomsko delo, , Fakulteta za računalništvo in informatiko, Univerza v Ljubljani, 2011.

[7] Repar, G., Ocena tveganj za informacijski sistem Ustavnega sodišča RS, (Organizacija in management informacijskih sistemov), Magistrsko delo, Univerza v Mariboru, Fakulteta za organizacijske vede, 2010.

[8] SIST ISO/IEC 27001 : 2013 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve

[9] Vehar, K., Projekt vpeljave SUIV v podjetje Alpina d. o. o., magistrsko delo, UM FOV, Kranj, 2012

BIOGRAPHY

Jože Šrekl was born in Loška Gora, Slovenia, in 1950. Assistant Professor in the Department of Technical Safety, Faculty of Chemistry and Chemical Technology, University of Ljubljana. He graduated from the Faculty of Natural Science and Technology, Department of Mathematics, completed his M.Sc. thesis in University of Zagreb, Faculty of Mathematical and Natural Sciences, PhD at the Faculty of Chemistry and Chemical Technology, University of Ljubljana, where he worked with the applications of statistical methods in safety and fire safety. He has participated in two international research, funded by the PHARE project, and two studies financed by the Ministry of Defense of the Republic of Slovenia. As the author of five published articles in major scientific journals worldwide, participated in three major international conferences and more conferences to international participation. Wrote university textbooks and a reviewer of several books, monographs and articles published in international journals. For more than ten years, he was Head of the Department of Occupational Health.

POBOLJŠANJE BEZBEDNOSTI INFORMACIONIH SISTEMA UPOTREBOM ISO/IEC 27000

Jože Šrekl, Andrejka Podbregar

Rezime: *Zadatak kompanije je da u velikoj meri obrati pažnju na bezbednost informacionih sistema. Neophodno je obezbediti sistem podrške organizaciji ukoliko želimo kontinuitet i efikasnost poslovanja. Pored bezbednosti koja se može postići putem tehnoloških mera predostrožnosti sa ciljem sprečavanja nametanja i zloupotrebe, potrebno je obratiti više pažnje na ranjivost i pretnje izazvane od strane korisnika. Ovde je reč o neželjenim pretnjama, koje su rezultat neispravnog načina rada ili nepoznavanja informacionog sistema. Važno je težiti smanjenju mogućih uzroka incidenata izazvanih nepravilnom upotrebom informacionih tehnologija, koja su uglavnom rezultat neznanja. Zadatak organizacije je da razmotri i identifikuje ranjivosti sistema i moguće pretnje. Svakodnevno se susrećemo sa rastućom količinom informacija u elektronskom obliku. Ostvarivanje bezbednosti informacionih sistema (IS) na radnom mestu podrazumeva mnoge korake koje kompanija mora preuzeti i sprovesti. Ispituje se ranjivost sistema, dok se javlja terorizam novog doba - sajber terorizam. U radu će biti reči o načinima smanjenja rizika i povećanja bezbednosti i zaštite IS. Ovde su takođe predstavljeni i mogući načini bezbednog korišćenja IS.*

Ključne reči: informacioni sistemi, upravljanje, zaštita, bezbednost.