Mechanics
Transport
Communications

Academic journal

ISSN 1312-3823
issue 3, 2007
article № 0178
http://www.mtc-aj.com

INFORMATION ASSETS SECURITY MANAGEMENT SYSTEM STANDARDIZATION ON RAILWAYS

Mirko DJAPIC, Ljubomir LUKIC
djapic.m@maskv.edu.yu; mdjapic@yahoo.com, lukic.lj@maskv.edu.yu; ljubomir.lukic@beotel.net

Mirko Djapic, Ph D, Assoc. Prof., Ljubomir Lukic, Ph D, Prof., Faculty of Mechanical Engineering, Dositejeva 19 36000 Kraljevo,
SERBIA

Abstract: *Use of information technology enables better communication of railways organizations with their environment. Under such conditions, railways organization information assets face serious security threats. Following this, the paper presents the information security concept and the ISO/IEC 27000 series standards that provide a harmonizing approach to development, implementation and maintenance of information security management systems (ISMS).*

Key words: *information security, ISMS, ISO/IEC 27001, ISO/IEC 17799.*

INTRODUCTION

Business today cannot be conceived without the implementation of information technologies. Information is becoming an important resource on which depend the organization's survival and development. Railways organizations are becoming more and more open, connecting their information resources with customers, suppliers and other partners. This leads to the emergence of numerous security threats such as computer fraud, espionage, sabotage, vandalism, fires, floods, etc. Damage to the organizations in the form of malicious code, computer hacking and denial of service are becoming an increasingly present phenomenon.

Russian Railways working on information security

Russian Railways company has announced the completion of several information security projects. Cisco and WatchGuard equipment and software connecting the railroad LAN to the Internet were installed at Oktyabrskaya and Kuibeshivskaya railways during one of the projects. In addition, RiskManager security assessment software was integrated into the information security monitoring system in the headquarters. It will let the central security department control information security in railway divisions. A separate project was conducted for Express-3 ticket-selling system. CompuLink experts developed suggestions on the information security system enhancement and its compliance with ISO 17799 and ISO 27001 international standard requirements.

(From: http://www.ospint.com/text/d/2618422/index.html)

Regardless of the format information is stored in, it has to be adequately protected. In order to provide adequate information protection all users must be familiar with the concept and necessary protection measures.

Information protection, preserving its confidentiality, integrity, and availability is becoming of primary importance. Information security is much more than using the appropriate technical solutions offered by contemporary information technologies. Because, as stated in [1] "If you think that you can solve your security problem by technology, then you understand neither the problem nor the technology".

Relying on the concept that information security is much more than the implementation of state-of-the-art technical solutions offered by information technologies, the developed countries (above all the United Kingdom through its national body for standardization BSI) have decided to develop appropriate standards covering this area. Thus, in the mid 1990-ties the first BS 7799-1 and BS 7799-2 standards emerged. The International Organization for Standardization (ISO) has taken over the development of these standards since the year 2000. together with the International Electro technical Commission (IEC) through a joint technical committee (JTC1).

This paper presents the information security concept and the ISO/IEC 27000 series standards that support it.

WHAT IS INFORMATION SECURITY?

Information: is a datum with specified meaning, that is, knowledge that can be transmitted in whatever format (writing, audio, visually, electronically or in another way).

Information can be:

♦printed or written on paper;

♦electronically stored (memorized);

♦transmitted by mail or electronically;

♦displayed on the corporation web site;

♦verbal – spoken in conversation;

♦knowledge– skills of the employees.

Information and their belonging data, as well as processes and systems (hardware, software, network, etc.) that are used for their generation, processing, communication, memorizing and access represent an important part of organization's **business assets** which need to be appropriately protected if one wishes to conduct business normally providing organization's survival and growth. This request becomes increasingly important due to the organization's distributed business environment where information is exposed to **vulnerability** due to numerous **threats** (Figure 1.).

Regardless of their nature, the information resources (information assets) (Table 1.) can have one or several of the following characteristics:

♦They are recognized at the organization level as an entity that has value;

♦They cannot easily be replaced without using resources such as: money, employees' skills, time, etc.

♦They constitute organization's identity without which organization's operation can be compromised

♦Threats to the information resources in an organization are:

♦Employees;

♦Low level awareness of the need for information protection (corporate culture)

♦Increasing networking and distributed data processing

♦Increasing complexity and effectiveness of hacking tools and viruses

♦E-mail

♦Fires, floods, earthquakes etc.

Main goals of information protection in an organization are to provide:

♦Business continuity, and to

♦Minimize risks from potential damage

This is achieved by preventing incidents and by reducing their potential impact.

Defining, implementing, maintaining and promoting the information security concept can be of crucial importance for achieving and maintaining competitiveness, financial means inflow, profitability, compliance with legal regulations and securing the organization's business prestige.

Information security is equally important to small and large enterprises, to public and private organizations. Connection between public and private computer networks and information sharing impede information access control. Under such circumstances, centralized controls are not effective. That is, implementation of technical solutions, appropriate equipment and products is not sufficient to ensure adequate information security management.

Information security is not exclusively the problem of information technologies (IT) but it is a "business" problem as well. The general consensus is that by implementing the appropriate technology only part of the information security problem is solved.

Today information security is achieved by implementing appropriate **controls**, relating to the security policy, business processes, procedures, organization structure, and hardware and software functions (system and application software).

Controls important for the organization from the legal standpoint are: a) information protection and confidentiality of personal data; b) safekeeping of organization's reports; c) observing the intellectual property rights. Controls that are in practice showing good results in implementation of the information security concept are: a) security policy; b) responsibility allocation for information security; c) awareness of the need for information protection, education and training of employees; d) correct data processing in applications; e) management of vulnerabilities of information resources; f) management of business continuity; g) management of security incidents and system upgrading

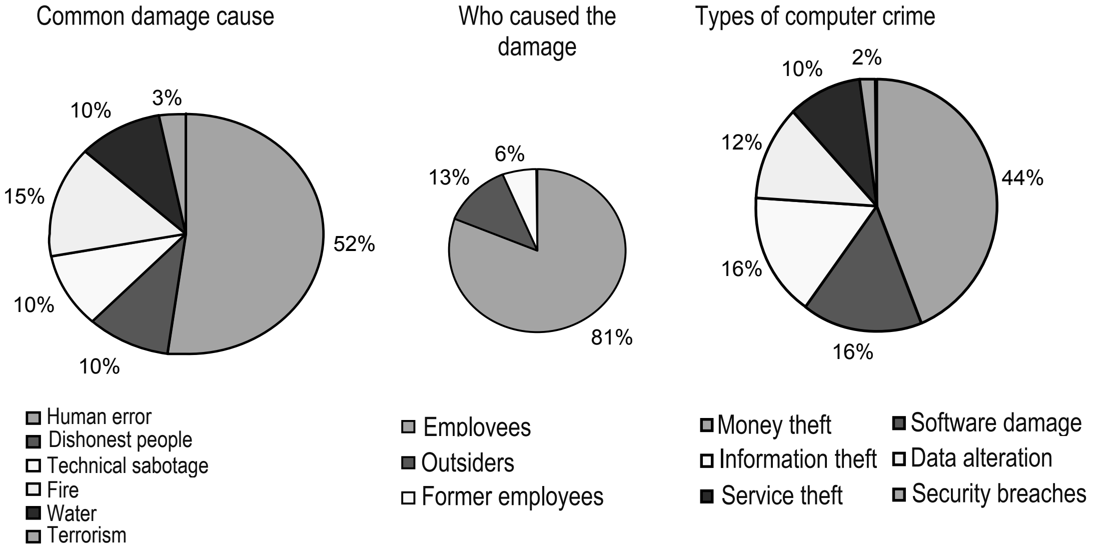

Fig. 1 Causes and types of computer crime (Adapted from [5])

Table 1 Information resources categories (assets) that should be protected

Information resources category (assets)	Examples:
Information	Data bases and data, system related documents, user manuals, training materials, operative and system procedures, continuity plans, record system
Software	Application and system, tools for software development
Physical resources – hardware (computer equipment)	Computer devices (processors, monitors, laptops, modems), communication devices (routers, switches, telephones), magnetic media (tapes, disks), other technical devices (power supply systems, cooling units, etc.)
Services	Data processing services, communication services
Personnel	Employees' knowledge and skills (technical, operative, marketing, financial, etc...)

WHAT ARE THE COMPONENTS OF INFORMATION SECURITY?

Information security includes application of protective measures for data being **processed**, **stored,** or **transmitted** against data loss (Figure 2.):

♦**confidentiality**,

(refers to the protection of certain data, i.e., information, from whatever intentional or unintentional disclosure to unauthorized personnel);

♦**integrity**

(refers to the preservation of accuracy and integrity of information and to the prevention of unauthorized alteration of its content)

♦**availability**

(relevant information is available in temporally acceptable terms to relevant subjects)

as well as the prevention of **integrity** and **availability** loss in the systems themselves.

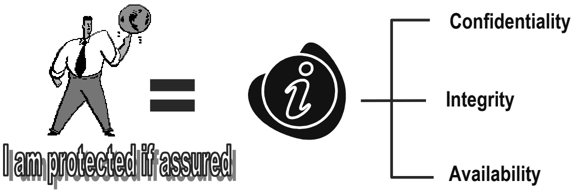

Fig. 2 Information security components

Information security is actually the risk management process. Security management should be part of the overall risk management, and information security is only one aspect of the overall organization security.

Risk management has to be a constant, continuous process, because risks themselves change, and on the other side, new risks are constantly generated as the result of the changing environment in which the organization is pursuing its mission. This means that it is necessary to periodically reviewed risks, threats and weaknesses of information resources. This precisely is the basis of the Information Security Management System (ISMS).

A harmonized process of establishing ISMS is presented in the ISO/IEC 27001:2005 standard. Establishing ISMS that complies with the ISO/IEC 27001 requirements has to be realized through a project which implies the implementation of methods and techniques of project management.

STANDARDIZATION IN THE AREA OF INFORMATION SECURITY MANAGEMENT

International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) have formed a joint technical committee JTC1 which has a permanent committee SC27 (ISO/IEC JTC1/SC27 "IT Security Technique") dealing with developing standards in the area of IT systems security. This committee has launched a new series of standards ISO/IEC 27000. This is the standards family on Information Security Management Systems (ISMS) planned to be developed in the next 5-7 years. It is planned that this series will include (Figure 3.):

♦ISO/IEC 27000 ISMS – Fundamentals and Vocabulary;

♦ISO/IEC 27001 ISMS – Information Security Management Systems requirements;

♦ISO/IEC 27002 (ISO/IEC 17799 after 2007. will become) - Code of Practice for Information Security management;

♦ISO/IEC 27003 - ISMS Implementation Guidance;

♦ISO/IEC 27004 – Information Security Management Measurements;

♦ISO/IEC 27005 – Information Security Risk Management;

♦ISO IEC 27006 – Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems.

Only two standards from this series have been published. These are ISO/IEC 27001:2005 and ISO/IEC 17799:2005.

Standard ISO/IEC 17799:2005 defines the best practice code in the area of information security. The entire standard is based on eleven security categories (chapters) which cover all the aspects of information security. These categories are:

♦Security policy;

♦Organization for information security;

♦Assets management;

♦Human resources security;

♦Physical and environmental security;

♦Communications and operations management;

♦Access control;

♦Information systems acquisition, development and maintenance;

♦Information security incident management;

♦Business continuity management;

♦Compliance with legal and other regulations.

Each of the above security categories defines security objectives as well as the controls that need to be implemented in order to reach these objectives. It is important to note that these controls are defined as the mode of risk management, implying policies, procedures, and guides, supporting organization structures that could be administrative, technical, managerial or legal.

In parallel with this standard, the ISO/IEC 27001 standard was also developed which defines the requirements that the information security management system has to comply to and according to which the certification of the ISMS is conducted. These requirements are based on the objectives and controls (best practice) defined in the ISO/IEC 17799 standard.

The entire information security concept defined in the ISO/IEC 27001 and ISO/IEC 17799 standards is based on the concept of risk management. Risk assessment is defined as the assessment of threats to information (threats that result in breach of confidentiality, integrity and availability of information) their impact on information and on the vulnerability of information and information systems, and the probability of their occurrence. Risk management is defined as the process of identification, control and reduction or elimination of security risks that could have an impact on information and information systems, which has to be financially justifiable.

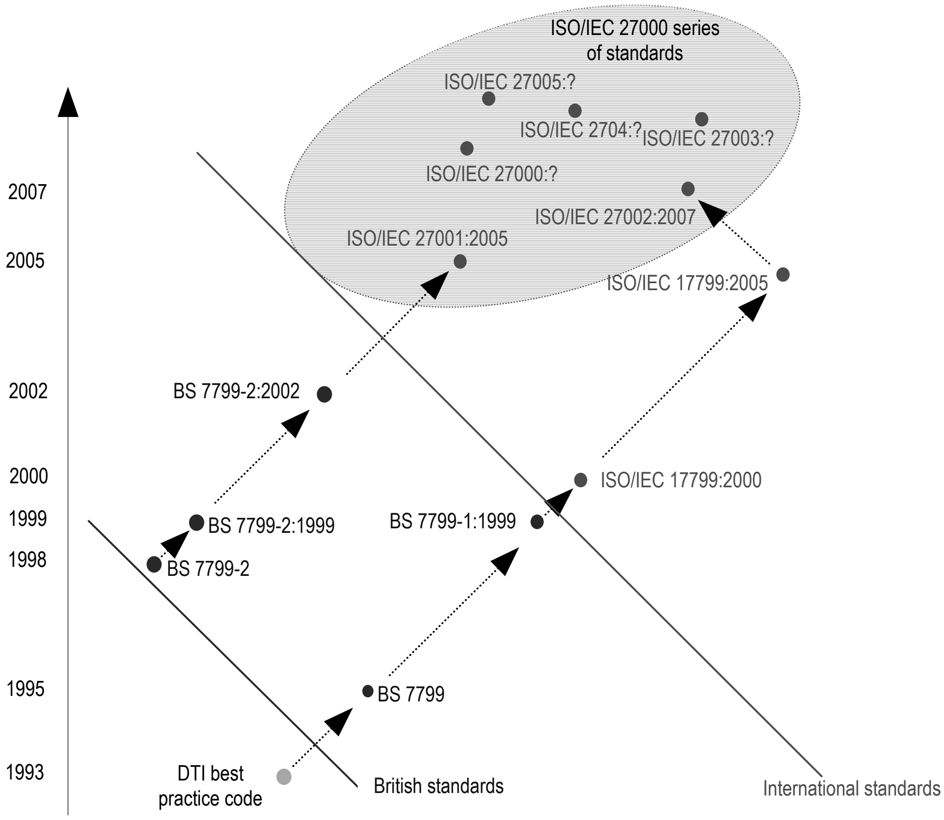

Fig. 3 Development of the ISO/IEC 27001 and ISO/IEC 17799 standard

CONCLUSION

Information technologies play a central role in developing and maintaining competitiveness of contemporary organizations. The introduction of the internet, intranet, e-commerce, etc., has significantly improved the ability of organizations to react quickly to constant changes taking place in the environment in which the organization is performing its activities. Without implementing these technologies the organizations can hardly survive on the market that is becoming increasingly global.

The opening of organization’s information resources toward the external world has also negative effects. Information and information resources (information, hardware and software) are exposed to numerous security threats such as computer fraud, industrial espionage, hacker sabotages, viruses, etc. Organization’s survival is directly related to its ability to protect its information assets. Therefore, concept of information security is becoming prominent.

Contemporary business practice shows that the information security problem is not exclusively the problem of information technologies, but it is more a "business" problem that has to be dealt with by the highest level of organization’s management. At its core is the risk management problem.

The ISO/IEC 27000 series of standards, i.e., standards ISO/IEC 27001:2005 and ISO/IEC 17799:2005 offer a harmonized approach to the management of risks that the information assets in the organization are exposed to through development, implementation and maintenance of Information Security Management Systems (ISMS).

REFERENCES:

[1] Kenning, M., Security management standard - ISO 17799/BS 7799, BT Technology Journal, Vol 19, No 3, July 2001, (pp 132-136).

[2] Humphreys, T., Plate, A., *An International Common Language for Information Security*, ISMS Journal, Issue 6, Jan 2006, (pp. 2-3).

[3] Vermeulen, C., Van Solms, R., *The information security management toolbox - taking the pain out of security management*, Information Management & Computer Security, Vol 10, No 3, 2002, (pp 119-125).

[4] Broderick, S., *ISMS, security standards and security regulations*, Information Security Technical Report IT, 2006, (pp 26-31).

[5] Solms, R., *Information security management: why standards are important*, Information Management & Computer Security, Vol 7, No 1, 1999, (pp 50-57).

[6] Fawaz, M., *Information security management systems* (power-point presentation), QMI seminar, Malaysia, 2004.

[7] ISO/IEC 27001:2005, *Information technology - security techniques - information security management systems - Requirements*.

[8] ISO/IEC 17799:2005, *Information technology - security techniques - code of practice for information security management.*

СТАНДАРТИЗАЦИЯ НА СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ РЕСУРСИ В ЖЕЛЕЗНИЦИТЕ

Мирко Дяпич, Любомир Лукич

Машинен факултет в Кралево,
СЪРБИЯ

Резюме: *Използването на информационната технология позволява по-добра комуникация на железопътните организации с тяхната среда. При такива условия информационните ресурси на железопътната организация среща сериозни заплахи за сигурността си. Следвайки това, докладът представя концепция за информационна сигурност и серия от стандарти по ISO/IEC 27000, които осигуряват хармонизиращ подход за развитие, приложение и поддържане на система за управление на сигурността на информацията (ISMS - СУСИ).*

Ключови думи: *информационна сигурност, ISMS, ISO/IEC 27001, ISO/IEC 17799.*