RESEARCH PAPERS
FACULTY OF MATERIALS SCIENCE AND TECHNOLOGY IN TRNAVA
SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA

10.2478/v10186-012-0019-0 2012, Volume 20, Special Number

INFORMATION SECURITY MANAGEMENT (ISM)

Jarmila ŠALGOVIČOVÁ [1], Vanessa PRAJOVÁ [1]

Abstract

Currently, all organizations have to tackle the issue of information security. The paper deals with various aspects of Information Security Management (ISM), including procedures, processes, organizational structures, policies and control processes. Introduction of Information Security Management should be a strategic decision. The concept and implementation of Information Security Management in an organization are determined by the corporate needs and objectives, security requirements, the processes deployed as well as the size and structure of the organization. The implementation of ISM should be carried out to the extent consistent with the needs of the organization.

Key words

information security, information security policy, asset management of organization, business continuity management, management of intrusion

Introduction

Information is inevitable in all kinds of entrepreneurial activities, and must be therefore protected as assets. Information security may be assured in various ways, including related policies, processes, procedures, organizational structures, software programs and hardware equipment able to eliminate many sources of safety jeopardising such as espionage, computer fraud and deceit, sabotage, vandalism, fire or water.

Requirements for information security should cover three areas:

- risks to the organization, including its strategy and objectives, its potential vulnerability and the likelihood of adverse events;
- legislation, statutory, regulatory and contractual requirements that the organization and its contractors must comply with;
- principles, objectives and business requirements for processing the information, that the organization must develop in order to refrain from business failures and to support its activities.

[1] Prof. Ing. Jarmila Šalgovičová, CSc., Ing. Vanessa Prajová - Institute of Industrial Engineering, Management and Quality, Faculty of Materials Science and Technology, Slovak University of Technology, Paulínska 16, 917 24 Trnava, Slovak Republic, jarmila.salgovicova@stuba.sk, vanessa.prajova@stuba.sk

Risk assessment

Risk assessment must include assessment of the risks size (risk analysis) and its comparison with the determined criteria. This work must be repetitive owing to the possible changes in the conditions of the company operation or with regard to the possible acceptability of risks.

The outcome of the risk assessment may involve:

- limitation of the risk occurrence;
- acceptance of risk and limitation of its occurrence
- reduction of the activities related to a given risk;
- delegation of the risk to another organization (insurance, suppliers).

Management of the organization must define information security policy in compliance with the requirements of the organization, applicable laws and regulations. The policy has to be officially approved, published and communicated to all employees and interested parties. At planned intervals, the policy must be reviewed and communicated to all stakeholders, especially if there have been changes that might threaten its suitability, adequacy and effectiveness.

Information security policy must have its owner, who, besides evaluating, keeps assessing the options of its improvement, including the following issues:

- feedback from stakeholders;
- results of independent reviews;
- state of corrective and preventive actions;
- results of previous reviews;
- changes in the organizational structure that might affect security of information;
- trends in information security vulnerability, including documented cases;
- recommendations for the responsible authorities.

If an organization does not dispose the information security experts, it should outsource external specialists, while involving and systematically training all interested managers, users, auditors, security employees and experts with expertise in such issues as insurance, legislation, human factors and risk management. Our experience shows that it is effective to determine the owner of each piece of property, as well as to systematically verify at planned intervals the safety system and the equipment used.

Special attention should be paid to the external stakeholders of the information security system involved in the risk assessment process, agree with them the process of assessing the potential risks as well as appropriate management and control mechanisms. The latter should cover:

- facilities that will be available to external stakeholders;
- access type to facilities (physical, logical via information, network connections);
- importance, value and criticality of the information provided;
- necessary checks of the information protection;
- identification of authorized staff dealing with information;
- importance of the information confidentiality and possible unavailability;
- seriousness of the potential failure of security measures;
- related legislative protection of information;
- involvement of cooperating organizations.

Asset management of organization

All company assets must be registered and inventoried, and must have an assigned owner responsible for its protection. The documentation must also include the information necessary to cure the crash.

The assets of the organization comprise:

- information (databases, data files, agreements and contracts, research results, training materials, audit results, operational instructions etc.);
- software files;
- technical equipment;
- services (computer and communication, heating, lighting, air-conditioning etc.);
- staff and their qualifications, skills and experience;
- intellectual property (reputation, image of organisation).

It should be underscored that high quality inventory of assets is an important entry to risk management. Rules for handling the property are also important for its security and efficient use, particularly regarding confidentiality, integrity and availability.

Operative management

Organization must ensure the proper and safe operation of information processing equipment, including identification of responsibilities and preparation of documented procedures for the execution of all activities including:

- processing and handling the information;
- backing up all the information;
- scheduling co-operation with other systems (especially when starting and finishing the activities);
- instructions for handling errors and dealing with unexpected events and contacts in unusual situations;
- instructions for safe disposal of incorrect results;
- procedures for restarting the system in case of failure.

Related operating procedures should be regarded as official documents which must be approved by management. This concerns particularly the changes to hardware and approved changes. Experience shows that one of the effective ways of reducing the risk of improper use of hardware is delegation of duties and responsibilities, particularly if the organization deals with an entire chain of issues from development and testing up to standard use.

Another effective measure preventing accidental or deliberate devastation of information is its systematic backup and re-verification, while taking into account:

- importance of back up information;
- need for creating backup copies and their integrity;
- extent and frequency of back up information in accordance with its criticality and the need of users;
- location of back up information (e.g. in-house or at a remote location) and its protection;
- options of re-storing the stored information, including its encryption.

These facts are related to the security of the entire information network, which can work either within the organization or across the world, using also publicly available services. The network managers must be responsible for:

- operation of the entire network rather than for the operation of computer networks;
- management of external equipment, including that at the beneficiary's site;
- data protection and integrity in the public network or wireless systems;
- suitable monitoring of the standard network activity, as well as the attempts to misuse it;
- development of technical security, protection and rules of using network, if necessary;
- development of appropriate operating procedures for data protection, documents, computer environment (e.g. disk) and system documentation from unwanted interference (modification, removal, destruction, disclosure);
- disposal of removed auxiliaries (discs, tapes, etc.);
- protection of the entire system documentation.

Control information access

Organization should establish, document, review and observe the policy of access to information, based on the business and security requirements, while clearly defining the rules for the information use and the rights of its users. Consideration must be given to:

- safety requirements of individual entrepreneurial entities;
- all information used and related risks;
- policy of providing information and principles of its authorization and classification;
- legislative requirements and related contractual requirements;
- requirements of management regarding access rights;
- requirements for periodic examination of access rights;
- revocation of access rights.

An important aspect of the development and utilization of any information system is its security including an operating system, infrastructure, applications, services, purchased products and developed applications. Prior to the formulation and development of system requirements, it is important to agree security requirements and consider potential business damage. Simultaneously, it is important to check the used operating software version, which must be verified by qualified professionals and authorized by management. Only authorized personnel should have access to the source code in case of necessary program changes. The implemented changes should be followed by technical reviews of software applications. Particular attention should be paid to the outsourced software.

Business continuity management

Business continuity management focuses on the consequences of adverse impacts and subsequent recovery after failures due to natural disasters, accidents related to equipment and those caused by bad intention, based on the identification of critical business processes and their impact on the standard operation as well as the analysis of their failure, which should include:

- understanding risks the organisation faces, probability of their occurrence and their impact on the operation;
- identification of all equipment crucial for business processes;
- understanding consequences of interruptions of activities due to failure of business safety measures;
- provision of appropriate insurances;
- introduction of additional preventive controls;
- provision of adequate financial, organizational, technical and environmental resources;

- guaranteeing the safety of workers;
- regular tests and innovation of equipment and implemented plans;
- assurance that business continuity management is a component of the organization's structure and strategy.

Compliance with legislation

Information security management may be subject to legal requirements; it should be therefore developed in co-operation with legislative advisors. Considered should be also legislative differences between states, as well as intellectual property rights, which may include:

- software products;
- parts of assets;
- licences;
- number of users;
- maintenance interventions;
- disposal of software and hardware;
- auditing system;
- copying information.

Law requirements may also concern proper documentation, records, developed software, patents, brands, personal information and cryptographic measures.

Conclusion

Statistics prove that the foreign information theft and abuse are becoming a profitable business worldwide. Perfect computer systems pose a significant barrier to illegal activities, yet **there is always a chance to hack and misuse a system.**

Organizations such as ISO, IEC, OECD and IEE have therefore prepared a wide range of standards, guidelines and instructions on how to implement information security management, e.g.:

- *ISO/IEC 27002: 2007 Information technology. Security techniques. Code of practice for information security management*
- *ISO/IEC Guide 73: 2002 Risk management. Vocabulary. Guidelines for use in standards*
- *ISO/IEC 13335-1: 2004 Information technology security techniques. Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management*
- *ISO/IEC 15408-1: 1999 Information technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model*
- *ISO/IEC 15489-1: 2001 Information and documentation. Records management. Part 1: General*
- *OECD Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security. 2002*
- *ISO/IEC TR 18044 Information Technology. Security Techniques. Information security incident management*

References

1. ISO/IEC 27002: 2007 Information technology. Security techniques. Code of practice for information security management
2. ISO/IEC Guide 73: 2002 Risk management. Vocabulary. Guidelines for use in standards
3. ISO/IEC 13335-1: 2004 Information technology security techniques. Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management
4. ISO/IEC 15408-1: 1999 Information technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model
5. ISO/IEC 15489-1: 2001 Information and documentation. Records management. Part 1: General
6. OECD Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security. 2002
7. ISO/IEC TR 18044 Information Technology. Security Techniques. Information security incident management

Reviewers:
Doc. Ing. Jana Šujanová, CSc.
Renata Stasiak Betlejewska, MSc. PhD.