Information Security System and Development of a Modern Organization

Wawak, Slawomir

Cracow University of Economics

October 2009

INFORMATION SECURITY SYSTEM AND DEVELOPMENT OF A MODERN ORGANIZATION

Sławomir Wawak , Cracow University of Economics

1. Application of the Information Security Management System

Information security management systems are increasingly applied in a number of sectors of the new, global, interconnected economy. They are used by production and service companies, businesses that provide information technology and telecom services, state administration authorities and local governments. Specifically, they are used in case of crime groups or as a means of securing illegal transactions. Intelligence services and governmental agencies cannot be ignored here either. Information security and information technology are world's fastest growing industry, and not surprisingly - one of China's fastest growing industries as well. In fact, the increasing computerization in both private and public sectors (despite heavy government control) makes China a market with huge potential for software development, outsourcing and security services, essential for economic growth and national security. China's rapidly developing software market however is yet to display its full potential.

One of the world leading suppliers of information security technology is a giant company, known for a long time as China Public Security Technology, Inc., (now operating as Information Security Technology Inc. - ISTI) is a case in point. The ISTI is a provider of integrated solutions for the public security sector not only in the People's Republic of China, but also throughout the world, and is specializing in controlling and ensuring security of information, providing public security information communication applications and Geographic Information Systems (GIS) software services globally[1].

Global controls to secure confidentiality and aimed at limiting access to data are especially critical in case of businesses that are involved in research and development of new technologies and products, companies that are linked to key industry sectors (e.g. oil refineries and power plants) authorities that organise tender procedures. Constant accessibility is of specific importance for information technology companies that provide services relating to websites and e-shops, offering e-mail support services or provision of Internet access, media houses and telecom companies.

Apart from confidentiality and accessibility, business and authorities also attach great importance to other attributes of information, for example: updateness, reliability, completeness, comparability, inambiguity, dependability, processibility, flexibility, efficiency, cost, response

Sławomir Wawak is an adjunct professor of Management at the Cracow University of Economics

[1] The Company has three segments: Information Security Segment, GIS Segment and Product Sales Segment. Information Security Segment includes revenues from information security related projects. GIS Segment includes the PGIS and civil-use GIS sales.

time, stability, detailness, addressability, usefulness, priority, value, ease of use, clarity, security [K. Woźniak, 2005, pp. 157-161].

Further to simultaneous occurrence of various needs, three directions of implementing an information security management system needs to be considered: controls securing against external actions, measures securing against internal actions, and preparation in case of an insufficient level of security controls.

Controls securing against external actions are related to introduction of limitations of physical and electronic access by persons from outside an organization, and also to implementation of tools recording contacts between the external environment and the company's information technology system. This may include instituting industrial security service, access cards, encryption protocols for data transmission, additional security controls for logging with the use of keys of tokens, etc.

Controls securing against internal actions refer primarily to employees. Following implementation of such controls, access to selected premises is limited, physical security controls securing stored information and limits on electronic contact within the company are introduced. Implementation of actions focused on employees may have a strong impact on their motivation level for work, therefore it shall be necessary to include changes in the incentive system, and also employee training will have to be carried out, making them aware of reasons for imposing such restrictions.

The third direction of ISMS development concerns preparation of plans in case of an insufficient level of security controls. Such a situation may occur as a result of underrating importance of threats, their wilful acceptance further to a low probability of their occurrence or impossibility of implementing costly security controls. Prepared plans may concern responses to threats, the sequence in which people, documents, and equipment are saved, quick recovery of the organisation's part following a breakdown.

It must be noted that application of the information security management system may have a positive impact on the organization's pace of growth, since it allows keeping confidentiality of certain types of information, while, simultaneously, facilitating flow of others. Consequently, the organisation should not suffer losses by business intelligence, and or to other costs of ineffective information management that are difficult to measure.

The third direction of ISAS development concerns preparation of emergency plans. Such a situation may occur as a result of under rating the importance of threats or the impossibility of implementing the costly security controls. Prepared plans may concern responses to threats, the sequence in which people, documents and equipments are noticed and first recovery of the organizations operations following a break down.

2. Features of the ISMS

The extent of an information security management systems of a security policy at the strategic level, risk estimation of threat occurrence, defining and implementing security controls aimed at eliminating such threats and also system monitoring with the use of internal audits and management reviews. It has been reflected within the structure of ISO 27001:2005 standard that counts of nine chapters. The first four include an introduction, a scope of the standard, normative references, and also terms and definitions. The key chapters relate to the principles of implementing and maintaining an information security management system, management responsibility, internal audit, management review, and ISMS improvement. That structure corresponds to other standards established by ISO which relate to management systems. Reasons behind distinguishing the last three chapters may however raise doubts, both in terms of the volume and their isolated contents. In ISO 9001:2000 standard a review follows as an item in the chapter on management responsibility, whereas audit is incorporated in the chapter on improvement and measurement, and it should be noted that these are the same system management tools in both standards.

Annex A constitutes the key part of the ISO 27001:2005 standard, which contains a list of controls divided into the following groups: security policy, information security organization, organizational asset management, human resource security, physical and environmental security, systems and networks management, system access control, information systems development and maintenance, information security incident management, business continuity management, and compliance management. The groups of controls are closely related to the contents of the ISO 17799:2005 standard, which presents detailed guidelines for implementing and monitoring of controls. It should thus be noted that there are numerous cases where the ISO 17799:2005 standard mentions an information system however in case of implementation of an information security management system it should be given broader interpretation, as an information system.

The ISO 13335 standard, which currently comprises five sheets, constitutes a background for implementing an ISMS, since it provides general knowledge about models and concepts of managing information systems. It presents a number of security aspects at various organizational levels: corporate, interdepartmental, departmental or in the information technology area. It contains both guidelines for the risk estimation methodology and also detailed principles for securing information systems.

When developing standards for management systems the International Organization for Standardisation complies with the principles of their compatibility and complementarily. Apart from ISO 27001, the most popular standards in that area also include systems of quality, environment or work safety management. Compatibility is reflected through application of similar methods and management tools, e.g. principles of supervision over documents and entries, development of organizational policies, performance of reviews of management systems, internal audits, identification of irregularities (or incidents), corrective and preventive measures. Such an approach facilitates simultaneous implementation of systems. It is worth noting, however, that in case of separate implementation of standards, the best solution for an organization is to first implement the quality management system that encompasses the entire company and introduces its employees to new working methods. Management systems developed by ISO supplement each other, thus providing for organization development towards a concept of total quality management (TQM).

It must be noted that application of the information security system management may have a positive impact on the organization's pace of growth since it allows keeping confidentiality of certain types of information, while, simultaneously facilitating flow of others.

3. ISMS and Organisation Development

An information security management system has a twofold impact on an organization. It provides for faster growth due to enhanced communication, on the one hand, and forces implementation of changes, both static and dynamic (organizational structure, processes, management tools), on the other.

The basic advantage from ISMS implementation for the majority of organizations consists not in increased data security, but in enhancement of communication. This is so because companies that have sensitive data, as a rule, apply security solutions that ensure a certain level of protection, usually a technical one. Problems relating to information flow, however, are difficult to measure for managers and therefore neglected.

Designing and implementing an ISMS requires an analysis of the communication system and indication of improvements that shall, at least, ensure its efficient operation, as a result of caring about continued accessibility and completeness of information. Other critical factors that do not directly stem from the requirements of ISO 27001:2005 include, among others, elimination of flow of redundant information, provision of updateness and reliability. The communication system that has been improved in that way shall provide employees with higher quality and speed in decision-making, which translates into better functioning of the organization and its growth.

The above-mentioned benefits stemming from increased information security reveal themselves especially in planning future activities, e.g. development of strategies, marketing campaigns, ownership transformation, mergers and acquisitions. Prevention of premature disclosure of information may provide for undisturbed execution of development plans.

Benefits that an organization achieves from implementation of an information security management system partially depends on the phase of its development cycle in which it finds itself. In the inception and youth phase there are problems relating to addressability and protection of access to information, because in case of a structure and division of responsibilities that have not been fully established each employee has knowledge about operations of the entire business, which may pose a threat in the event of their transfer to competition. On the other hand, however, lack of clearly defined ownership of information assets forces central decision-making by the owner which may delay growth.

With the growth of business and an increasing amount of information it becomes necessary to design communication channels to ensure access to necessary data for the employees. Otherwise, there will occur problems relating not only to access, but also to updateness. Such a situation shall create a risk of making erroneous decisions.

A stabilised organization should enhance its relatively stable communication system. Therefore, cost of production and access to information, its efficiency or value will be the key factors in this phase. Decisions taken on the basis of analysis of such issues may increase communication effectiveness and that of the entire organization.

ISMS implementation shall have an impact on the structure of an organization as well. Particularly interesting may be changes that are necessary in case of modern structures that use advanced information systems, like virtual, fractal, network or learning organizations.

A virtual organization may operate owing to development and popularisation of information technology. Intangible assets are of key importance in attaining objectives and are supported with information assets. A virtual organization is usually made up of a number of organizations operating together towards achieving a specific or more assignments. Its creation may be triggered by spinning off all processes from organization, except for information processes or by co-operation conditions that prevail in the market. In the latter case it is hard to indicate a central entity since, depending on undertaken projects, that role may be given to various parts of the organization. Features distinguishing a virtual organization may include (Managing the Enterprise, Zarządzanie przedsiębiorstwem, 2005, p. 116.):

- broad use of information technology in relationships with suppliers, customers, associates, and also seeking to limit or eliminate other communication and data exchange techniques, e.g. preference to electronic payments,
- sales carried on the Internet only through the use of: offers presented in websites, promotion on WWW and through e-mails, points of sale on the Internet, use of Internet-based orders and forms,
- development of the offer on the basis of results of surveys into the customers' needs carried mainly on the Internet and also offering possibilities of adjusting the product to specific requirements of a person placing an order, opinions of buyers are material input data for product design,
- dominance of informal relationships with suppliers, the majority of core employees are external associates; in case of larger organizations there may be a permanent group of administration staff,
- intangible resources are mainly used and processed, with qualifications and skills being the source of a competitive advantage, therefore it is important to develop a proper corporate culture, carry a continued process of training and improvement.

In a virtual organization the used information technology tools have numerous publicly available interfaces that support sales or ensure access for associates. Some of the central organization's knowledge must be disclosed to business partners to be used by them in their work. But they have a loose relationship with the company and are often involved in a number of organizations at the same time. Further to that there is a significant difficulty in securing documents that are handled by business partners. In case of orders executed by business partners for the customers (e.g. consulting companies), lack of full feedback information about the progress of work may be dangerous. The major objectives of the implemented ISMS must thus include: legal security of information available for business partners and development of the communication system that shall ensure complete feedback information. This will allow limiting the risk of a slowdown in growth as a result of departure of one or more associates. Increasing the efficiency of a communication system will provide for better identification and satisfaction of customers' needs.

A fractal organization is made up of numerous parts having a similar structure and operating principles. They have significant freedom of operations, however, they are continuously controlled by a superior entity that establishes and transmits primary principles of operations. Features distinguishing a fractal organization may include (Managing the Enterprise - Zarządzanie przedsiębiorstwem, 2005, p. 152):

- it operates using self-organizing teams of employees operating in a self-similar structure, in which relations between elements are based on mechanisms of inheriting objectives and permanent control and steering actions,

- it is characterised by a high level of adaptability attained owing to a continued optimisation of resources and processes, and also by flexibility related to modern forms of employment. That is why it best performs in a turbulent environment with rapid changes,

- teams of employees shall have a maximum level of independence, which requires the employer's trust, loyalty of employees and also high aspirations and willingness to perform,

- owing to full availability of information and with its free flow ensured, the processes of employees learning are effectively carried; this requires communicative skills, abilities to learn, and also willingness to share knowledge and flexibility.

Application of modern technologies of remote communication causes threats to information security. Self-organization of fractals has to be in line with implementing specific security solutions. A free flow of information may thus pose a threat to the company. However, it is the corporate culture based on trust in employees may be an obstacle to implementation of constraints in the communication system. It must be taken into account at the stage of designing the ISMS, otherwise effectiveness of the organization may decline following system implementation.

Network organizations are sets of organizationally and legally independent units that undertake long-term co-operation to achieve an effect of synergies. Most often they form companies operating within strategic groups that provide complementary products or have similar capabilities. Their major distinctive features include (Managing the Enterprise - Zarządzanie przedsiębiorstwem, 2005, p. 170):

- repeatedness and long-term nature of exchange,

- strong co-ordination of operations,

- joint decisions taken relative to resources,
- shared-knowledge about how business partners operate.

In case of network organizations, threats relate to the necessity of developing information channels between organizations and the risk of information leaking through to competition when the network is broken. Departure of an employee may pose a material danger if he/she has information about operations of other companies in the network. Then, legal controls, e.g. competition ban to establish an employment relationship with a competitive organization may prove to be insufficient. This problem may be solved through implementation of the ISMS across all organizations and have that system integrated through risk estimation and implementation of controls not only within individual companies, but also at the boundary between them.

Within a learning organization, the corporate culture is focused on acquiring knowledge. Any experience is used to develop new knowledge. It is characterised by openness, a possibility of discussing things, presenting diverging opinions. It requires applying an open information system that is accessible by all employees. Personal enhancement, autonomy of individuals, instability, superfluity and diversity of knowledge, as well as mutual trust are necessary conditions for that.

Such assumptions shall significantly make implementation of the information security system difficult, as it is a system that imposes constraints on information flow, encourages to limit superfluity. Broad access of employees to knowledge may pose a threat, however, prevalence of creative chaos may lead to disregard for certain controls. The major problem may be the stability of an ISMS in view of frequent changes of operating methods due to dynamic introduction of new organizational solutions. Therefore, it becomes necessary to design the system in such way that it will not limit that dynamism.

An information security management system within a learning organization must thus be based on efficient information technology applications that shall ensure permanent access to information, its automatic indexing and searching. In the situation of superfluity of information, information technology tools that have been properly configured may significantly contribute to increased efficiency.

4. Summary

Development of a modern organisation depends on accessibility, proper flow, and also provision of security of information. Broad use of information technologies shall improve operational efficiency of a company, but at the same time it exposes it to additional threats relating to access on part of unauthorised persons.

Quite recently, in fact in the fall of 2009, the world's premiere consulting firm, Deloitte, ranked highly and awarded high prize to China Information Security Technology, Inc., (CIST), a leading total solutions provider of digital security, geographic information, and hospital information systems. Companies are considered technology companies if they either develop proprietary technology that contributes to a significant portion of their operating revenues, manufacture technology-related products or devote a high percentage of revenue to technological R&D.

Nonetheless, awarding the world's leading manufacturers of leading total solutions provider of digital security, as it has been shown earlier, three major challenges remain – that of compliance with the ISO 27001:2005 standard. The ISO 27001:2005 standard does not suffice, since its requirements do not cover all major features of an information system. Its advantage, however, is inclusion of most important aspects that an organization should focus upon, and also easier integration with other systems based on ISO standards. Implementation of information security management should thus be a starting point for the reorganization of information systems in terms of growth acceleration.

Bibliography

ISO/IEC 17799:2005 Information Technology – Security Techniques – Code of practice for information security management, ISO, Genewa, 2005

ISO 27001:2005 Information technology – Security Techniques – Information security management systems - Requirements, ISO, Genewa, 2005

ISO TR 13335-3 Information Technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security, ISO, Genewa 1998

Woźniak K., SIM jako instrument wspomagania zarządzania strategicznego w firmie, Akademia Ekonomiczna w Krakowie, Kraków 2005

Zarządzanie przedsiębiorstwem w turbulentnym otoczeniu, red. R. Krupskiego, PWE, Warszawa 2005