The Importance of Information Security Management in Crisis Prevention in the Company

Wawak, Slawomir

Cracow University of Economics

2010

6th International Symposium on Business Administration
GLOBAL ECONOMIC CRISIS AND CHANGES
Restructuring Business System: Strategic Perspectives for Local, National and Global Actors
The Conference Proceedings

THE IMPORTANCE OF INFORMATION SECURITY MANAGEMENT IN CRISIS PREVENTION IN THE COMPANY

Sławomir Wawak, Ph. D.

Cracow University of Economics

Key words
information security management, crisis prevention, tools and techniques,

Abstract
Management information system can be compared to the nervous system of a company. Its malfunction may cause adverse effects in many different areas of the company. Information Security Management is understood as tool of the information confidentiality, availability and integrity assurance. An effective information security management system reduces the risk of crisis in the company. It also allows to reduce the effects of the crisis occurring outside the company.

1. Information security management system

Information security in today's organizations, be understood as a domain of professionals who install and configure equipment and software. According to many presidents and directors, their companies are very well protected by firewalls, antiviruses, data encryption and password systems. However, as practice shows, the technical security will never be sufficient to deter those interested in gaining organization assets.

Requirements of information security management system proposed in ISO 27001:2005 are assumed as a base of considerations in this article. Although the standard is not a complete source of knowledge of this subject, however it presents a very clear structure of information security issues, as well as highlights the need for a process approach. Considering the implementation of security without a comprehensive analysis and recognition process is doomed to failure, as shown by R. Anderson [1] and K. Mitnick [6].

Information system is a multi-layered structure, which enables the transformation of input data into output using procedures and models, while computer system can be defined as part of an information system, which has been computerized [5]. Information system can be compared to the nervous system. To malfunction in one place can cause failure of the entire organization and its exposure to risk of loss or a fall. Therefore, maintaining high performance information system, including the appropriate level of security, may have a direct impact on how organizations respond to crises.

The three main properties of an information system that are important to ensure information security are confidentiality, availability and integrity. Confidentiality is defined by ISO 27001:2005 as "the property that information is not made available or disclosed to unauthorized individuals, entities, or processes" [4]. Most computer systems are designed with a view to functionality, the need for confidentiality is noticed by the developers in the later stages of software design. In view of continuously developing technologies, such as cloud computing, ensuring confidentiality is becoming increasingly challenging. No less important is the preservation of organizational procedures on confidentiality. In the last year

the media reported on several cases of their violation by experienced intelligence personnel or prosecution [7].

Issues with information availability, understood as "being accessible and usable upon demand by an authorized entity" [4], are not usually seen as a problem of the whole company. Lack of access to data is easily explained to the leave, the lack of electricity, a virus, or missed key. Some people ignore even company's website breaches, treating them as *signum tempori*. Availability of information is one of the factors affecting the ability of companies to maintain business continuity. Loss of the business continuity usually means heavy financial losses, the loss of the image, and even the need to close. It can be particularly dangerous for the company using technology which requires continuous operation of the production line.

A third main property of information system security is the integrity, that is to say "safeguarding the accuracy and completeness of assets" [4]. It may be considered at a technical level. Then it concerns on the structure and configuration of network devices and applications. However, problems of integrity is mainly related to the activities of workers collecting and processing data. Failure to comply with integrity may cause delays in decision-making by management or lack of actions to minimize the effects of existing threats.

Apart from mentioned properties, business and authorities also attach great importance to other attributes of information, for example like: updateness, reliability, completeness, comparability, unambiguity, dependability, processibility, flexibility, efficiency, cost, response time, stability, detailness, addressability, usefulness, priority, value, ease of use, clarity, security [8].

The ISO 27001:2005 states three aspects of information security: organizational, technical and information technology. This approach covers the entire company, not only the IT department. Standard 16 distinguishes areas of control. Areas related to organizational aspects are: security policy, organization of information security, asset management, human resources security, operational procedures and responsibilities, service delivery management, incident management, business continuity management, compliance, whereas the areas of technical and information technology are: physical and environmental security, system planning and acceptance, protection against malicious and mobile code, back-up, network security management, media handling, exchange of information, electronic commerce services, monitoring, access control, information system acquisition, development and maintenance. A full list of areas and the controls is shown in table 1.

Table 1. Control areas in ISO 27001:2005

Area of control	Groups of controls
Security policy	• information security policy
Organization of information security	• internal organization • external parties
Asset management	• responsibility for assets • information classification
Human resources security	• prior to employment • during employment • termination or change of employment
Physical and environmental security	• secure areas • equipment security
Communications and operations management	• operational procedures and responsibilities

	• third party service delivery management • system planning and acceptance • protection against malicious and mobile code • back-up • media handling • exchange of information • electronic commerce services • monitoring
Access control	• business requirement for access control • user access management • user responsibilities • network access control • operating system access control • application and information access control • mobile computing and teleworking
Information systems acquisition, development and maintenance	• security requirements of information systems • correct processing in applications • cryptographic controls • security of system files • security in development and support processes • technical vulnerability management
Information security incident management	• reporting information security events and weaknesses • management of information security incidents and improvements
Business continuity management	• information security aspects of business continuity management
Compliance	• compliance with legal requirements • compliance with security policies and standards, and technical compliance • information systems audit considerations

Source: based on [4]

Information security management system in ISO 27001:2005 is designed to enable its integration with quality management system, environmental management system and other systems based on the concept of a process approach. In practice, it is much easier to implement ISMS, if an organization has already implemented a quality management system based on ISO 9001. For one thing, employees have a higher qualification to work in such a system. Secondly, some management techniques are common to both systems.

The main link between these systems is the use of PDCA cycle (Plan - Do - Check - Act). ISMS uses the same tools as the other systems, such as audits, corrective and preventive actions and management review, but supplements them with particular information systems techniques. In addition to compatibility with the standards ISO 9000 and 14000, information security management system maintains consistency with ISO 19011, ISO 13335, and technical safety standards.

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 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 depend 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 taking erroneous decisions.

A stabilized 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.

2. Crisis in the organization

The company may face a crisis due to external or internal causes. Analyzing the crises resulting from external causes can be distinguished, in terms of range: industrial, national or international crisis.

Industry crisis that may be caused, inter alia, by changes in consumer preferences, the emergence of new technologies, regulations. It transmits itself directly to the companies with a small range of product diversity. A properly functioning system for collecting information about markets and changes in technology can allow to react in advance to the symptoms of the crisis.

National crisis may result from political, economic or environmental reasons. Enterprises realize it through the financial markets (difficulty in obtaining funding for

activities), changes in the level of sales and exports. The impact of this type of crisis can be reduced through sound financial management in the enterprise, as well as efficient financial information monitoring system. International crisis affects the company as a national crisis. However, its causes may lie outside the country in which the organization operates.

The internal crisis is associated with the processes of business development. It occurs when the former methods of business management cease to function properly. Based on the model L. E. Greiner, can be distinguished crisis of leadership, autonomy, control and bureaucracy [3]. Another common cause of internal crises in companies are failures that result from insufficient competence of top management, the improper use of methods and techniques, as well as undeveloped internal communication. Occurrence internal crisis can be accelerated or intensified by the crisis surrounding the organization.

Results of the study on communication processes in enterprises show that 60-80% of managers activity at all levels of management is communication. Efficient communication allows to spread information, coordinate activities, resolve conflicts and make decisions. Factors that increase organizations vulnerability to crisis threats include some of the pathologies of the information system, for example: differences in perceptions of the facts by the staff, distortion of information, lack of understanding of transmission of information, differences in language (professional vocabulary, idioms), over-interpretation, too much information, the occurrence of disturbances in communication (noise), lack of confidence, excessive filtering of information [2]. These pathologies can cause: improper information gathering, incorrectly performed analyses, decision-making based on incomplete data, misunderstanding of financial and strategic position of the company, failure to detect early signals of crisis.

3. ISMS tools to help prevent crises

Methods and techniques described in ISO 27001 standard are similar to those in ISO 9001. However, different manner and additional purposes of using these tools should be noted. The main tols of ISMS are:

- management review,
- corrective actions,
- preventive actions,
- incident management,
- risk assessment,
- risk treatment plans,
- compliance metrics,
- internal audit.

Management review. Management review is a regular meeting of executives dedicated to the functioning of the system. The main reviews are held several times a year, but short meetings even several times a month. Reviews allow to gather information, enable information comparisons and entail discussion between representatives of the organizational units. In this way the review causes that each participant better understands the situation of the company. Management review promotes the understanding of relations between different parts of the organization. Understanding those relations enables managers to more accurate detection of the problems.

Corrective actions. The aim of corrective actions is removal of non-compliance and incidents causes. These actions are taken based on information about identified non-compliance. Information security manager is responsible for the proper conduct of actions, While the employees according to their competencies are responsible for causes removal.

Quick removal of causes makes possible to minimize adverse effects, as well as immune company of a given type of causes.

Preventive actions. Preventive actions serve to detect and remove potential causes that could entail non-compliance or incidents. Their carrying requires involvement of all employees in order to identify potential problems. Procedures of running these actions is the same as in the case of corrective actions. Identification of the causes allows to find further causes of problems and better understand the organization and its environment. Moreover, removal of causes will imply that there won't be any adverse effects. Preventive actions are more difficult to implement, but they are more efficient (no losses).

Incident management. Detection of undesired events and quick response to it, is the goal of incident management. In addition, it provides information for corrective action. Identification and reporting of incidents is the responsibility of every employee. This tool increases the workers' awareness and sensitivity to the problems occurring in the company and its environment.

Risk assessment. Risk assessment is the periodic review of risk factors and identification of new factors. General assessment is usually done once a year. Besides it, during the year are carried out a number of minor assessments. Conducting risk assessment immediately after the identification of changes in risk factors provides the information necessary to take preventive action and update risk treatment plans.

Risk treatment plans. Risk treatment plan is a set of instructions followed in the event of a risk factor. The organization should make plans on the basis of risk assessment, audit reports and information from the outside. Valuable source of plans are simulations. Current and possible to implement plans should be practised, because when a problem occurs, there is usually no time to learn instructions. The employees who are able to recognize triggers, can automatically take action to reduce the impact of the causes that could entail a crisis in the company.

Compliance metrics. Compliance metrics are a set of metrics to monitor the functioning of the system. Not only the computer system, but the whole organization should be monitored. It is possible to create a measurement system based on the assumption BSC, which will set up an early warning system. Using precise metrics allows earlier detection of irregularities. However, the high accuracy of measurement increases costs of measurement.

It should be noted that the use of individual tools has little influence on the prevention of crises in the organization. It is necessary to use a coherent system to achieve this effect.

Internal audit. Internal audit is a tool for monitoring specific areas of business and processes. Its main objective is to improve the information system. This is achieved through cooperation between the auditor and auditee. A secondary purpose is non-compliance detection. Audit perfectly complements the other methods because it uses less formal, flexible approach. This makes it possible to detect risks that are not identified by other tools.

4. Summary

Development of modern organizations depends on the availability, proper flow, and ensure information security. Extensive use of information technology improves the efficiency of the enterprise, but exposes the organization to additional risks.

The implementation of the information security management system is a process that is by far more complex than the implementation of the quality management system due to the large number of factors that may affect its effectiveness. It thus becomes necessary to ensure highly qualified staff, who have skills, not only in the field of information technology, but

also know the principles of how to implement management systems on the basis of ISO standards well.

It should be noted, that well-implemented information security management system has the ability to reduce the risk of crisis in the organization, thanks to tools that could early detect its causes.

Literature:

[1] Anderson R., Inżynieria zabezpieczeń, Warszawa: WNT, 2005, ISBN 83-204-3069-0
[2] Bylok F., Bariery komunikowania interpersonalnego w przedsiębiorstwie i sposoby ich przezwyciężania w społeczeństwie informacyjnym, in Zarządzanie firmą w społeczeństwie informacyjnym, edited by A. Stabryła, Kraków: EJB, 2002, p. 93, ISBN 83-885119-26-3
[3] Greiner L. E., Evolution and revolution as organizational grow, Harvard Business Review, July/August 1972, ISSN 0017-8012
[4] ISO 27001 Information technique. Security technique. Information security management systems. Requirements, Geneva: ISO, 2005
[5] Kisielnicki A., Sroka H., Systemy informacyjne biznesu, Warszawa: Placet, 2005, s. 17, ISBN 83-85428-94-1
[6] Mitnick K., Simon W., Sztuka podstępu. Łamałem ludzi, nie hasła, Gliwice: Helion, 2003, s. 21, ISBN 83-7361-116-9
[7] Pendrive zgubiony czy ukradziony, http://wyborcza.pl/1,76842,6144849, Pendrive_ zgubiony_czy_ukradziony.html, 9.01.2009
[8] Woźniak K., SIM jako instrument wspomagania zarządzania strategicznego w firmie, Kraków: Akademia Ekonomiczna w Krakowie, pp. 157-161, dissertation

JEL Classification M15
http://www.aeaweb.org/journal/jel_class_system.html

Contact – email
wawaks@uek.krakow.pl