Managing Sustainability?
Proceedings of the 12th Management International Conference
Portorož, Slovenia, 23–26 November 2011

THE ROLE OF INFORMATION SECURITY IN QUALITY OF MANAGEMENT

Sławomir Wawak, Cracow University of Economics, Poland, wawaks@uek.krakow.pl

ABSTRACT

The importance of access to information in organizations constantly grows. On one hand, there is high demand for complete information, and secondly it is desirable to prevent information overload. Proper information management affects not only the quality of managers work, but through effects of their work also affects quality of all employees in the organization. Therefore, there is high importance of proper information system construction. The article discusses one aspect of such a system – information security.

Keywords: quality of management, information security, information systems

1. Introduction

Over the last several years an access to timely, accurate and complete information has increasing impact on the work of managers Information system built by companies and government offices are to provide complete data necessary to make a high quality decision. The focus on making decisions based on facts and analysis in various areas of management increases. It can be noticed in quality management systems, and concepts of corporate government. However, as noted already in 1999 by P. F. Drucker (2009, 105), error made by designers of information systems is to provide data, not information.

The rapid development of Internet and other information technologies has caused that modern manager has access to vast amounts of data which is not itself able to process due to the inadequate use of advanced information systems. As a result, the quality of decision making, instead of rising – falling. Analyses are conducted on the basis of random and incomplete data, and in some cases, instead of time-consuming analysis, managers rely on their intuition.

Information overload therefore affect the decision-making in two ways. On the one hand, an employee may not be able to identify what information is most needed to him, which is a result of a wide range of available data beyond limits of human perception. On the other – too much information may lead to incorrect inefficient use them (Farhoomand, Drury 2002, 127).

Research conducted by the A.F. Farhoomand and D.H. Drury indicated that 2/3 of

managers are often faced with information overload (37% every day). The main effects of improper functioning of information systems in organizations are a waste of time, deterioration of performance, reduced work efficiency and frustration. The authors suggest remedies in the form of filtering information, eliminating redundant data sources, the delegation of tasks, the categorization of the importance of information (Farhoomand, Drury 2002, 128-129).

Taking into account the growing importance of information management, these solutions should be considered as insufficient and not enough comprehensive. There is a need of integrated approach to the reconstruction of the information system, including changes that will ensure proper flow of information. In this article, because of the scope of publication, and the complexity of the problem, there will be discussed only one of the elements that make up these solutions – the information security management system and its potential impact on the quality of the manager's work.

2. Information security management system

Information security in today's organizations, can 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 experience has shown, technical security will never be sufficient enough to deter those interested in gaining organizational assets.

The requirements of the information security management system proposed in ISO 27001:2005 are assumed as a base for the considerations in this article. Although the standard is not the complete source of knowledge on this subject, it does, however, present a very clear structure of information security issues, as well as highlighting the need for a process approach. The implementation of security without a comprehensive analysis and recognition process is doomed to failure, as shown by R. Anderson (2005) and K. Mitnick (2003).

An information system is a multi-layered structure, which enables the transformation of input data into output, using procedures and models, while the computer system can be defined as part of an information system, which has been computerized (Kisielnicki, Sroka 2005, 17). The information system can be compared to the nervous system. A malfunction in one place can cause the failure of the entire organization and its exposure to the risk of loss or a fall. Therefore, maintaining a 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 infor-

mation 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" (ISO 27001 2005). Most computer systems are designed with a view to functionality, and 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 years the media reported several cases of their violation by experienced intelligence personnel or prosecution.

Issues about information availability, understood as “being accessible and usable upon demand by an authorized entity” (ISO 27001 2005), are not usually seen as a problem of the whole company. Lack of access to data is easily explained away by leave, the lack of electricity, a virus, or missed key. Some people even ignore company's website breaches, treating them as signum tempori. The availability of information is one of the factors affecting the ability of companies to maintain business continuity. The loss of business continuity usually means heavy financial losses, the loss of the image, and even the need to close. It can be particularly dangerous for a company using technology which is required for the continuous operation of the production line.

The third main property of information system security is integrity, that is to say, “safeguarding the accuracy and completeness of assets” (ISO 27001 2005). It may be considered at a technical level. Then it concerns the structure and configuration of network devices and applications. However, problems of integrity are 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 a lack of actions to minimize the effects of existing threats.

Apart from the properties mentioned, 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, and security (Wozniak 2005, 155-161).

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. The 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 and 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.

3. Quality of management

Quality of work should be seen as an integral component of quality of life. It is the issue of growing importance in today's job market. It is bound by different authors with satisfaction from work, subjective well-being of workers (Connell, Burgess, Hannif 2008, 62). But these is a simplified approach. In an attempt to operationalize this concept, it should be noted that the quality of work consists of two dimensions: the quality of management and the quality of performance. In terms of the gurus of Total Quality Management, the first is domain of the managers, and the second – the employees. It was assumed that impact of the quality of management on quality of products can amount even 90% (Galetto 1999, 18).

Aware creation of quality of management should include (*Współczesne* 2008, 114):

- development of policies and planning of the quality of management,
- control of the quality of management,
- improvement, e.g. by improving the quality of managing human resources, optimizing the use of property the organization, a high level of human capital management.

The objectives should be (*Współczesne* 2008, 114):

- complete satisfaction of customer needs and expectations,
- implementation of the requirements for owners and employees,
- meet the expectations of other stakeholders.

T.J. Chemmanur, I. Paeglis and K. Simonyan noticed, that high quality of management is not only important for the company and its customers, but also in other dimensions. The high reputation within the competence of managers and their ability to manage work teams have an impact on the ease and cost of access to finance for business development (Chemmanur, Paeglis, Simonyan 2009, 1045).

The quality of management denotes "the extent to which a set of inherent features of a co-ordinated action, concerning the management of an enterprise and its supervision, satisfies the needs and expectations (that have been established, commonly accepted or the compliance of which is mandatory): an enterprise, its customers and other interested parties" [T. Wawak 2001, s. 73]. Figure 2 presents relations between the quality of management and other dimensions of quality within the organisation.

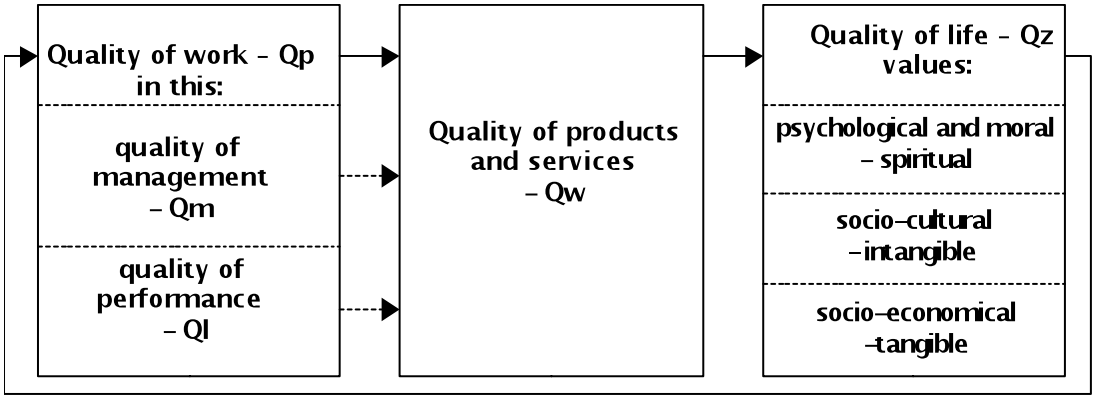

Fig. 1. Combination of quality of work, products, and life

Source: (Wawak 2001, 73).

The quality of management (Qm) is a component of the quality of work (Qp) understood as the extent to which performed work and its results (deliverables) impact the development of the performer, organisation, customer, and the environment. It depends on the manner in which performed tasks are organised (Qm) and the attitude of the person performing them (Ql). Given such an understanding the quality of work directly affects the quality of products (Qw) delivered by the organisation, and indirectly the quality of life (Qz).

A low quality of management means, among other things: unclear directions of development, ineffective methods of monitoring, insufficient knowledge of managers about training needs, lack of knowledge of the market reality, non-adjustment of the management style to situations. Selected consequences of low quality management have been presented in more detail in Fig. 2.

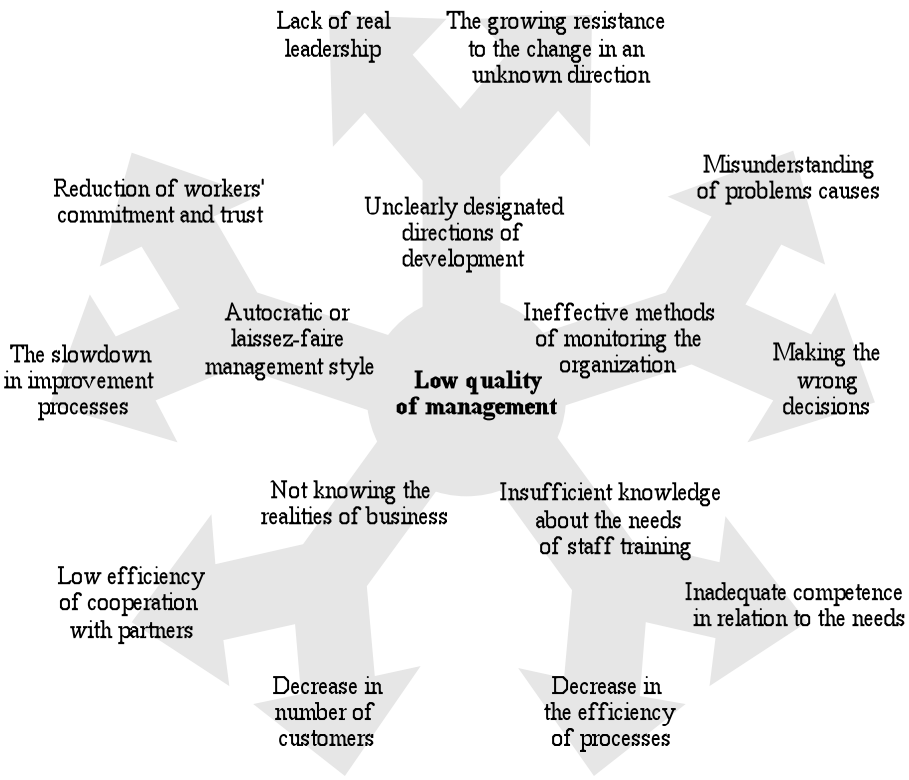

Fig. 2. Consequences of low quality management

An inappropriately selected style of management will slow down the development of an organisation. A lesser faire approach by management will make employees in individual organisational units take decisions on how to cope with difficult situations themselves. These actions are not, however, co-ordinated, which limits their effectiveness. Such a situation discourages, lowers commitment, and impedes processes of change. In addition, employees' confidence in the organisation is lowered, the effect of which is increased departures among the staff. In the case of applying a clearly autocratic style that sometimes is perceived as a proper one in crisis situations, the scope of employees' responsibilities is decreased in practice which makes them less committed in actions that go beyond their duties. Therefore, enhancement processes may slow down.

An unclear setting of the organisation's development directions makes employees, wishing to properly perform their assignments, consult their management more often. The lack of a clear vision from the management, or even improvising when faced with an adverse condition in the enterprise, makes work difficult, lowers its effectiveness, and also affects the level of acceptance for change among the staff. Frequent changes of direction and irregular actions pursued by the organisation's management brings about growing opposition against individual changes. Also, the gradual lowering of the management's authority and increasingly apparent lack of real management within the organisation is of importance for the

company's future.

Enterprises that have extended systems monitoring all signs of their operations should be capable of predicting the occurrence of threats much earlier. A crisis situation is a test for such systems. Inappropriately adopted criteria, measures, indicators, or their measurement may result in a crisis that, despite an expanded and costly tool, will not be predicted sufficiently early or the applied measures will turn out to be inappropriate and ineffective. In the first situation, the measurement system itself requires improvement, whereas in the second the procedures of responding in crisis situations also necessitate such enhancement. It is worth noting that not all authors perceive having a monitoring system as tantamount to the need of having emergency procedures. Incorrect monitoring may result in the misunderstanding of the real causes of problems, and also lead to making incorrect decisions.

An erroneously operating monitoring system may also be one of the reasons for limited knowledge of the management with regard to the realities of business operations. Another reason may be the conviction of the company's management about the correctness of the hitherto policy which is to justify lack of interests in changes in the environment – managers become hostages of their previous successes and do not perceive the need for development and changes in the way of management. The competition takes advantage of such a situation, winning over customers. Apart from obvious internal consequences for the organisation, relations with business partners also suffer , which means the enterprise loses its allies on the market.

Misunderstanding the company's situation combined with ignorance of the employees' abilities may lead to incorrect decisions with respect to staff education. This may be seen when they are not sent on training courses or when they are sent on courses that have not been preceded by an analysis of actual needs. Failure to detect such errors may prevent the development of the organisation until the proper skills have been acquired.

The quality of management is perceived as one of the key factors in a self-perfecting organisation (e.g. one that seeks implementing a quality management concept). W. Edwards Deming pointed out that 80% of the success of undertaken actions depends on it (Latzko, Saunders 1998). The selected consequences of low quality management that have been reviewed are also indicative of its importance for the organisation's development.

4. Impact of information security on the quality of work

An effective information system should comply with the following criteria in terms of information security:

- provide employees with access to necessary updated and reliable information that is required for their job positions,
- eliminate information that is redundant for the job position to prevent information overload,
- limit access to confidential information, including the prevention of drawing conclusions on the basis of a large number of non-classified information,
- have a high capability of recovery following the occurrence of adverse events or human actions,
- ensure the company's communications with the environment on the basis of assumptions concerning confidentiality, availability, and the integrity of information.

In a modern knowledge-based organisation, the high efficiency of incorrectly selected security measures of such a system may have an adverse impact on the quality of work. It happens when the system is designed without regard for the needs of employees in certain organisational units to have extensive knowledge about the enterprise's operations. A similar impact may be exerted by the implementation of changes without previously ensuring the full understanding of the employees of the necessity to use security measures. Such mistakes result in the creation of an atmosphere of excessive confidentiality, raising concerns among employees about the confidentiality of topics discussed in conversations, blocking communications between divisions and organisational units, and also a decline in trust in the organisation.

Seeking to ensure the accessibility of information, and also the continuity of operations in a situation of personnel changes, results in intense pressure on the formalisation of knowledge. This happens especially where extended information technology systems collecting data are implemented. Employees may therefore be additionally charged with documenting their knowledge. Practice shows that the usefulness of documentation thus prepared is negligible, since there is growing discouragement among the employees who prepare it to share such knowledge. On the other hand, their successors do not wish to devote time to reading extensive instructions – since access time to formalised knowledge is too long.

A properly designed and implemented system of managing information security may however affect the improvement of the quality of work. Enhancement of the integrity level, especially through the provision of complete (but without necessary elements) and updated information has a direct impact on the improvement of the quality of decisions made. Facilitating and ensuring the constant provision of information and data necessary for the

employees may increase the quality of their work, and also affect the level of their commitment. In a well-designed system, confidentiality should not be put as its major goal. In many organisations issues relating to internal confidentiality may be solved through appropriately worded clauses in contracts of employment, patent proceedings, or other legal solutions. Application of simple, transparent, but effective solutions with regard to confidentiality allows for the understanding and acceptance from employees. In such a case, technical and organisational security measures used to safeguard confidentiality may primarily be applied to relations with the environment, and also communication channels with business partners.

5. Framework project of applying the information security management system to improve the quality of work

A framework project supports a proposed way of implementing an information security management system (ISMS) and defines its construction. It presents implementation assumptions and tasks, and also points out an implementation methodology. The purpose behind the preparation of a framework project is to facilitate system implementation. The implementation procedure complies with the requirements of ISO 27001:2005, since the system that has been implemented pursuant to the prepared recommendations could be certified for its compliance with the said standard.

The organisation's management should adopt objectives relating to the implementation of the information security management system. Under the proposed concept, those objectives may include, among others:

- enhancement of the level of work quality,
- improvement of the information system in the organisation,
- increased accessibility of the organisation for partners and customers,
- provision of transparency of the organisation's operations.

The objectives should be made operational for a specific organisation in which the system is to be implemented. Dates and measures for assessing the extent of execution of individual objectives should be adopted.

A project team should comprise of top management in the organisation, managers of organisational units, IT specialists, and persons working in the security areas (e.g. secret registry, cash desk, server room). A quality manager (or an information security manager – depending on the adopted terminology) should be a member of the project team. Depending on the size of the organisation, it may be useful to set up to the following working groups:

1. IT security group – it analyses susceptibility and IT threats and prepares proposals of security measures,
2. technical security group – it deals with access to individual premises, including security areas,
3. departmental groups – they identify susceptibility and threats and propose solutions with regard to their core operations.

The project's scope should be defined both in terms of its objects and assignments. In terms of its objects, the project should comprise of all organisational units. As concerns its assignments, it should utilise the preparation and implementation procedure of the system described in Clauses 4.2 and 4.3 of ISO 27001 (*ISO 2700*1 2005, 9).

The procedure of preparing and implementing the information security management system has been described in clauses 4.2 and 4.3 of the standard (*ISO 27001* 2005, 9). It is made up of the following steps:

- defining the scope and boundaries of the ISMS,
- defining the ISMS policy,
- defining the approach to risk assessment,
- defining the risks,
- analysis and evaluation of the risks,
- identification and evaluation of risk treatment options,
- selection of controls,
- approval of all residual risks,
- obtaining authorisation for system implementation,
- preparation of a statement of applicability,
- development of a risk treatment plan,
- implementation of the risk treatment plan,
- implementation of security controls,
- defining the ways of measuring effectiveness of security controls,
- training of employees and associates.

The scope of the information security management system may not be freely defined, since it has to take into account the nature of operations pursued by an organisation. It is a mistake to subjectively or objectively limit the system that may cause its incomplete efficiency. The office management usually imagine, at the outstart, that the information security system will operate in the server room and the classified information bureau. Such a solution, however, would not include the number of job positions that are responsible for observing the

confidentiality or maintaining the continuous access to the information. The system should thus encompass the entire local borough council office, together with subsidiary organisations that perform local council works.

A good solution is to integrate the ISMS with the quality management system. There are a number of similarities between the two systems, such as the structure of documentation, at the top of which there is the ISMS policy. Its task is to define the major directions and principles of operations with regard to the provision of information security. From the point of view of strategic management, the policy may be treated as an element of strategy concerning the proper functioning of the information system. Such an approach, in the case of an integrated management system, allows for the easier management of many policies pursued in the office.

The development of the risk evaluation method is a key stage of designing the information security management systems. The ISO 27001:2005 standard does not point to any specific method, leaving some freedom in this respect. Such an approach is justified, since systems are implemented within different organisations. A proposal of the method is, however, included in the ISO TR 13335-3:1998 standard. Although it is limited to information technology systems, it may easily be adopted to a broader category such as an information system. The method must be prepared in such a way that it will provide for its multiple repetition and ensure the comparability of results. It should take into account not only legal requirements, but also those relating to the operations pursued by an organisation. The method must contain criteria that will allow for the definition of acceptable levels of risks, and on that basis, taking a decision about acceptance.

The ISO 27001:2005 standard requires risks to be defined in four steps:

1) identification what assets (information, hardware, etc.) are in the organisation in terms of ISMS implementation and who is responsible for them,
2) identification as to what could pose a threat to such assets,
3) identification of susceptibilities, or weaknesses of such assets that may be used by threats,
4) identification of the consequences for the assets that may occur in the event of threat occurrence.

The standard does not clearly indicate that threats and susceptibilities should be identified individually for each type of assets; however, auditors who certify systems are unenthusiatic about methods in which susceptibilities have been defined in groups. Risk identification is a time consuming activity and requires the participation of representatives from all the or-

ganisational units. Due to this, its optimum form includes training sessions combined with workshops.

Risk analysis is performed on the basis of the identification results. Its purpose is to show the losses that a default on confidentiality, accessibility, accuracy, or the integrity of assets may cause. Next, the likelihood of the occurrence of incidents that default on security and losses should be indicated, taking into account the currently applied security controls. Based on that, it is possible to estimate the risk level and take decisions on whether it is acceptable, or whether it is necessary to undertake additional preventive actions.

The standard proposes four solutions: the introduction of security controls, knowing the acceptance of risks, risk avoidance or their transfer to other organisations, e.g. insurers. The choice of security controls is facilitated by a list of over 100 proposals that has been presented in the standard implementation, which should be considered. The list has been prepared on the basis of information security management principles published in the ISO 17799:2005 standard.

Acceptance of residual (acceptable) risk by the management and an implementation approval constitute a passage from the design stage to the implementation stage of the information security management system. A statement of applicability of the ISMS, which is the outcome of the completed design stage, contains a description of the selected and implemented security controls, and also of any possible reasons for excluding certain security controls recommended by the standard.

Research conducted by the author in several local government offices has shown that technical security controls are used at a good level. Unfortunately, organisational security controls are at a satisfactory level. This is so because the implementation of technical security controls is the responsibility of an information technology officer, who has the relevant qualifications, whereas the organisational security controls are the responsibility of all employees. The implementation of such security controls will require substantial changes in the organisation's culture.

Due to that reason the implementation phase should be accompanied by a series of employee training courses. Their purpose is to acquaint employees with the new ways of the work organisation and to explain the reasons for introducing changes. Next, there comes the development and implementation of the risk treatment plan that will define the actions that need to be undertaken, their sequence, and the positions that are responsible for the introduction of changes should be indicated. The further stage includes the implementation of security controls provided for in the statement of acceptability, and defining the way of measuring

their effectiveness. The measurement should allow not only for the assessment of system operations in the future, but also the results of comparisons of changes in time.

REFERENCES

Anderson R. 2005. *Inżynieria zabezpieczeń*, Warszawa: WNT.

Bylok F. 2002. Bariery komunikowania interpersonalnego w przedsiębiorstwie i sposoby ich przezwyciężania w społeczeństwie informacyjnym. In: *Zarządzanie firmą w społeczeństwie informacyjnym*, ed. A. Stabryła. Kraków: EJB.

Chemmanur T. J., Paeglis I., Simonyan K. 2009. Financial and Investment Policies, and Asymmetric of Information. *Academic Journal Management Quality* 44: 5.

Connell J., Burgess J., Hannif Z. 2008. Job Quality: What does it Mean, What does it Matter? Comparison between Australia and the UAE. *International Journal of Employment* 16: 1.

Drucker P. F. 2009. *Zarządzanie XXI wieku – wyzwania.* Warszawa: MT Biznes

Farhoomand A. F., Drury D. H. 2002. Managerial information overload. *Communications of the ACM* 45: 10.

Greiner L. E. 1972. Evolution and revolution as organizational grow, *Harvard Business Review* July/August.

ISO 27001 Information technique. Security technique. Information security management systems. Requirements. 2005. Geneva: ISO.

Kisielnicki A., Sroka H. 2005. *Systemy informacyjne biznesu*, Warszawa: Placet.

Latzko W. L., Saunders D. M. 1998. *Cztery dni z dr Demingiem – nowoczesna teoria zarządzania.* Warszawa:WNT.

Mitnick K., Simon W. 2003. *Sztuka podstępu. Łamałem ludzi, nie hasła*, Gliwice: Helion.

Wawak T. 1998. *Jakość pracy a jakość życia.* In: *Polityka jakości polskich przedsiębiorstw w dobie integracji europejskiej.* Conference papers, Vienna.

Wawak T. 2001. *Zarządzanie a jakość pracy i życia*. In: *Zmieniające się przedsiębiorstwo w zmieniającej się politycznie Europie*. vol. 4. Kraków:Wydawnictwo Informacji Ekonomicznej.

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

Współczesne paradygmaty nauk o zarządzaniu. 2008. ed. W. Kowalczewski. Warszawa: Difin.