THE IMPACT OF POSITIVE ORGANISATIONAL CULTURE VALUES ON INFORMATION SECURITY MANAGEMENT IN THE COMPANY

JPM
Journal of Positive Management
Vol. 7, No. 1, 2016, pp. 87–98
© Copyright by
Wydawnictwo Naukowe
Uniwersytetu Mikołaja
Kopernika
ISSN 2083-103X

http://dx.doi.org/
10.12775/JPM.2016.006

Joanna Chmura

Nicolaus Copernicus University in Toruń,
Faculty of Economic Sciences and Management, Torun, Poland

e-mail: jchmura@doktorant.umk.pl

Abstract

Objective: The purpose of this article is to identify the positive values of the organisational culture, which have an impact on the effectiveness of information security management in the company.

Methods: The study was performed based on a case study. The study was divided into two stages. The first stage consisted of conducting an interview with a person responsible for the information security in the studied company. While the second stage assumed obtaining the opinions of employees regarding the organisational culture and the positive values influencing the information security in the company. Based on the literature review, a survey questionnaire was prepared, which was used in the survey. The study was conducted in a company employing 35 people.

Conclusions: The article highlights the important role of the positive values of the organisational culture, which impact the information security management in the company. Positive values have a big impact on maintaining the appropriate level of information security in the company.

Originality/Value: The analysis of the obtained results shows that cultivating positive values in the company impacts the effectiveness of information security management. The study suggests that the development of positive values in the company creates not only the positive atmosphere at work, but it also affects the observance of procedures and rules in the field of information security.

Keywords: information security, organisational culture, positive behaviour, information security management

Paper type: Case study

1. Introduction

The information is increasingly recognised as a basic product, without which most of the today's businesses cannot function. Unfortunately, in the world of new technologies, in which we live, the information is much more vulnerable than ever before. Storing and processing large amounts of data in the electronic form creates a lot of doubt about the information security. Therefore, in recent time, the issues related to the information security gained on importance, both among practitioners and scientists.

The recent reports on information security indicate that the number of threats increases from year to year, and the employees become the main source of the attack. This trend may be mainly due to the fact that the companies have focused their practice of information security mostly on the technical issues. This situation forces the today's companies to pay greater attention to the organisational issues related to the information security, like increasing the involvement of employees in order to understand the essence of the information security better.

Already in 1982, T. Deal and A. Kennedy showed that the organisational culture is one of the most important factors, which determines the success or failure of the company. The organisational culture shapes the values and behaviour of the employees. There's no denying that it affects the operational activity of the company and the effectiveness of the information security practice in the company. However, for several years, the information security becomes the major concern of almost every enterprise. Initiation of the information security practices in the organisational culture is a very difficult process to implement, as it requires undertaking many actions at different organisational levels.

The article aims to identify the positive values, which influence the effectiveness of information security management. Due to the complexity of the issue, the study was conducted based on the case study. The various characteristics of the organisational culture were analysed, which impact the attributes of the information security, i.e., confidentiality, integrity and availability. The analysis of the obtained results constitutes the foundation for further studies in the field of behavioural determinants of the information security management in the company.

2. Information security and organisational culture

2.2 Information security

Information technology in today's companies play an important role, therefore it can be assumed that the information security must be a key element of modern planning and the company management. This type of security for a long time has been largely driven by the increasing growth of electronic transactions and the continuous development of the Internet. It is generally accepted that the information security means the protection against a wide range of threats in order to ensure (ISO 27002):

- operation continuity,
- minimisation of the risk and maximisation of the return of investment,
- business opportunities.

The main objective of the information security is to ensure the confidentiality, integrity and the information availability (Chang Ho, 2006). Confidentiality means the property, in which the information is not made available or disclosed to unauthorised persons. Integrity means the property, which ensures accuracy and completeness of information and the methods of its processing. While the availability ensures that the authorised people have access to information and the associated assets always when it is needed (ISO 27002:2013).

The information security is used for the protection of all valuable information resources and mitigation of threats for the information from various sources (Szczęsny, 2012). In general, information security management is directed at the creation and maintenance of the optimal information security level in the company. The mere concept of information security management is based on the control of the obtained, produced and processed information in the structure of the given company. Therefore, the information security management system should be integrated with the complete company structure, and at the same time adapted to its business needs.

According to the World Research on Information Security (EY 2015), in which 1755 companies from 67 countries participated, the biggest problem concerning the information security involved phishing (44%) and malware (43%). The list of other hazards increasing the risk level in the field of information security is presented in Figure 1.

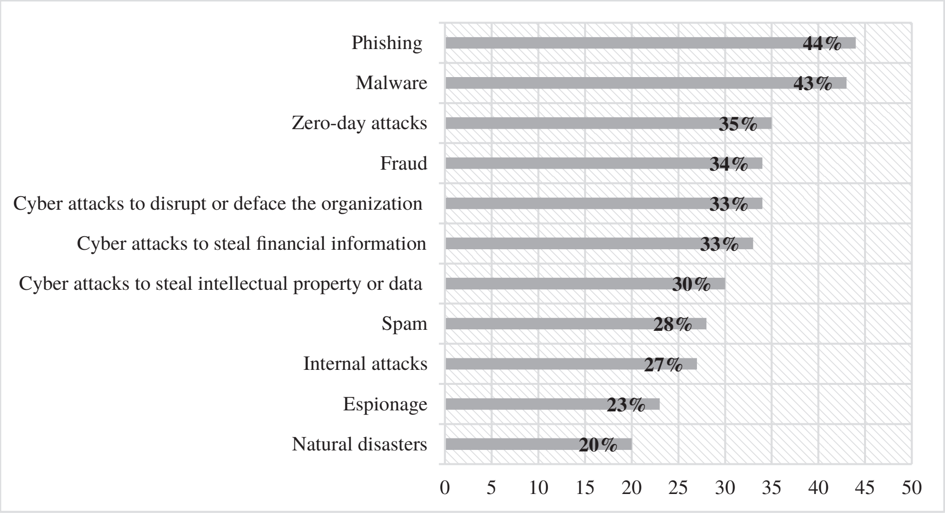


Figure. 1.
The list of threats increasing the risk level in the field of information security

Source: EY's Global Information Security Survey 2015.

The study results also show that most problems regarding the information security is caused by different kinds of negligence on the part of employees (Figure 2, 3).

The analysis of the study results forces the undertaking of the appropriate organisational measures regarding the information protection. The acceptable level of information security can be implemented and maintained only by the appropriate control set. Guidelines concerning the implementation of the information security management system are specified by the ISO 27001:2013 standard. The standard was mainly created to develop the common rules, which would allow the companies to develop, implement and effectively assess practices in terms of information security management. The scope of the standard covers the issues concerning the development of the employees' competence and different types of technical measures used to protect information from the computer intrusions (ISO 27001). The complexity of the content, included by the ISO 27001 standard, does not provide the absolute information security, but undoubtedly constitutes the foundation for the companies to develop, implement, monitor and measure the information security management system.

Figure 2.
The main sources of attack in Poland in 2015

Source:
Report PwC 2016, p. 10.

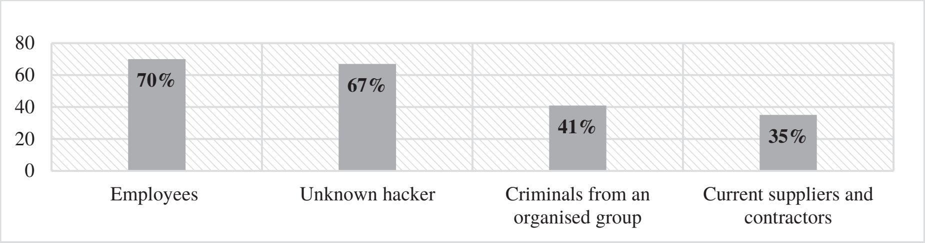
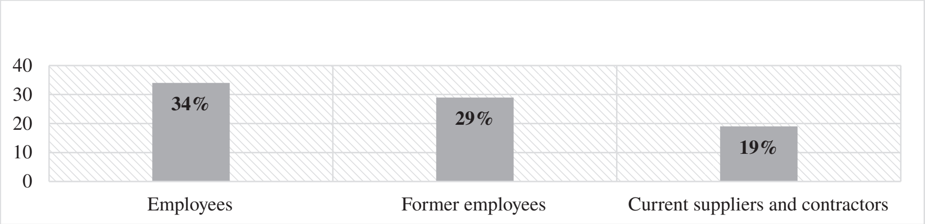


Figure 3.
The main sources of attack in the world in 2015

Source:
Report PwC 2016, p. 10.



Today's reality shows that the research in the field of information security should not focus only on the technical issues, because the studies in this scope will be subject to constant changes. The information security is not only a technical problem, but also a social and organisational one.

2.3. The positive aspect of the organisational culture

The organisational culture for many years has generated interest among the scientists. It constitutes a kind of phenomenon, which decides, next to strategy and structure, on the creation, development but also about the collapse of the company. The organisational culture is a resource, which is not only difficult to define, but it is also hard to attribute it with certain effects or conditions (Koźmiński et al., 2009).

The very concept of the organisational culture is multifaceted, which includes several categories of phenomena, including (Koźmiński et al., 2009):

- values – culture means values prized in the organisation, which are strived for by its members and employees, both individually and collectively. The values also relate to the way of functioning, interpersonal relations, or respecting the formal procedures;
- standards and patterns – that is, ready-made patterns of behaviour, which are used by the organisation members in certain situations;
- symbols – elements emphasising the sense of community, which constitute the understandable representation for everyone, both of the values, as well as the standards and patterns. Symbols can be both tangible (company logo, décor, organisational costumes), and intangible (important events, annual rituals).

The organisational culture is generally a set of values, standards, or views shared by a group of people, which determine their behaviour (Mikuła, 2000). The specificity of the culture is a kind of "organisation personality", the more original the culture, the stronger the personality.

The culture is also controlled by signals from the environment, among others, by the national and professional culture, experience of the direct work environment, or participation in the social communication. This kind of external conditions become an independent entity, which is also one of the most important determining factors, what is the most important for the organisation success – behaviour of its employees (Glińska-Neweś, 2010). Organisational behaviour never occur in a vacuum. They are the result of the personality of the given employee and the environment, in which it occurred. Because of the occurrence of differences between people and the variety of situations, in which a man faces in the work situation, usually it is difficult to predict such behaviour. The situation becomes even more complicated, when we realize that the way the employee behaves is determined by the way he perceives the situation he is in. To do this, it is worth familiarising with the key factors of the environment, which affect the employees' behaviour in the workplace, i.e., properties of the job, behaviour of the supervisors, organisational policy, or the atmosphere in the team. The behaviour being the result of the organisational culture usually tend to be authentic and sincere, because they result from the real beliefs and views of employees.

In the context of the information security management, the organisational culture can have a huge impact on the information security, that's why it should reflect the positive attitude to the whole system of information security management within the whole organisation (Vroom and Von Solms, 2004). Many authors rightly stress that the security is related not only to technology, but most of all to management. Without profound changes in the organisational culture, which has a direct impact on the security practices, none actions in this scope have a chance of success. Therefore, analysing the specifics of the problem it is worth adopting the concept of the positive organisational culture, which is based on several assumptions concerning the values expressing the faith and beliefs on what is important and right. The positive organisational culture consists of four groups of values reflecting the positive approach to the functioning of a man and employee (Glińska-Neweś, 2010):

- the pursuit of happiness (honesty, generosity, justice, respect for the truth, courage),
- striving for excellence and over-mediocrity (excellence, responsibility, commitment, rationality, trustworthiness),
- possession and use of the positive, creative energy (openness, pro-activity, adaptability, creativity),
- feeling good emotions (respect, trust, cooperation, loyalty, respect for organisational traditions).

The positive organisational culture can be a source of the company's strength, which proves the competitive advantage.

3. The impact of the positive values on the information security – the analysis of a case study

3.1. Methodology of research

The prepared and conducted study was aimed to identify the respondents' opinion on the selected issues on the scope of information security and organisational culture. A particular attention was paid to the aspect of positive values, which impact the effectiveness of the information security management.

The study was conducted in a company, which according to the classification belongs to small businesses. The company conducts the activity in the specialised design, employing a total of 35 employees.

The study was divided into two stages. The first stage consisted of interviewing a person responsible for the information security. In the studied company this function was played by the IT manager. The thematic areas of the interview related to the selected issues contained in Annex A of the ISO 27001 standard.

The second stage was to conduct the surveys among the employees. The study used a survey questionnaire, which was developed based on the literature studies. The survey consisted of 7 closed questions with a selected list of answers, both of the single and multiple choice.

3.2. Analysis of results

3.2.1. Stage I

The first stage of the research allows to get to know the opinion of the specialist for security, in this case the IT manager regarding the issue of the information security in the studied company. It results from the obtained information that the risk analysis was conducted in the company with the inventory of the computer systems. In the company also the information security policy was developed, containing the basic definitions of information security, goals and the importance of the information protection. The document was published and communicated to all employees. The IT manager confirmed that he cyclically performs the processes related to the information security according to the previously established rules. He has also stated that he make an inventory of all IT assets included in the company. On the issue of security of human resources, the owners put a lot of emphasis on training of employees in the field of information security. Training takes place periodically, they concern not only the technical issues, but also the organisational and social ones, in order to mitigate different risks. The building, in which the company operates, is subject to monitoring. On the other hand, the authentication of inputs and outputs is done using cards with a digital ID, which is owned by every employee. The record of the data media is conducted in the company. The access control to the information systems takes place based on the formalised process of awarding logins, passwords and permissions. Because of the financial capabilities of the company, the development of information systems is somewhat limited. The respondent underlines that all incidents related to the information security are reported by employees at the time of detection.

The analysis of the information security condition in the studied company performed based on the interview with a person responsible for the information security showed that the level of security is high. Despite some financial constraints in the company, mainly due to the nature of the conducted activity, great importance is paid to the issue of security and protection of information. The owners of the company are aware of the nature of the threats, both those related to the information systems, and those arising from the employees. The level of information security which has been specified in the company created the basis for further research, this time in the behavioural aspect.

3.2.1. Stage II

The general analysis of the information security in the studied company showed that the security system is at a high level.

The second stage allowed to obtain the opinion of employees on the level of information security, organisational culture prevailing in the enterprise and the values, which influence the effectiveness of the information security management. The data obtained from the survey showed that more than half of the respondents (74%) admits that they pay a lot of attention in the company to the information security and it is at a high level, the remaining 26% of the respondents think that there are a few areas from the information security, which should be improved. In order to diagnose the employee awareness in terms of the information security, the respondents were asked to answer the question: Is there the division according to the resource classification in your company? The analysis of data shows that almost (83%) respondents know and understand the division according to the resource classification. The obtained result only confirms that the employees are aware of the fact that the loss of confidential information is associated with the financial losses, but also the image borne by the company. Analysing the issues of the information security level and awareness of the employees in terms of information security, the respondents were also asked about the threats for the information security including the division into risks:

- external – generated mainly outside the company, including the risks related to the loss, damage or disability of the performance of certain operations on the data sets,
- internal – created inside the company, which result from the awareness or unawareness of the employees,
- random – natural disasters, which affect the state of information security, e.g., fire, flooding a building, in which the data carriers are located.

The distribution of the obtained results is presented in Figure 4.

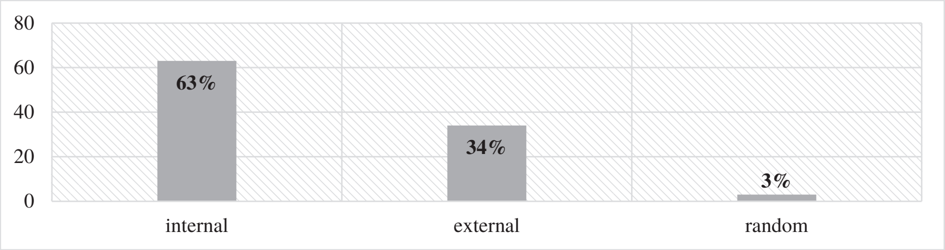


Figure 4. Sources of threats for the information security

The study results underline that the human factor is the weakest link in the process of maintaining the appropriate level of the information security.

The further part of the survey concerned the issues concerning the organisational culture and values, which impact the effectiveness of the information security management system. As part of this analysis the respondents were asked to give answers to the questions, which distribution is presented in Figure 5, 6, 7, 8.

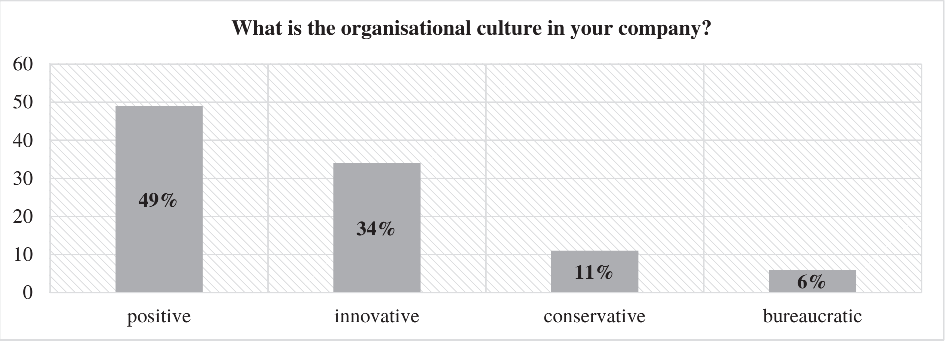


Figure 5. Type of the organisational culture

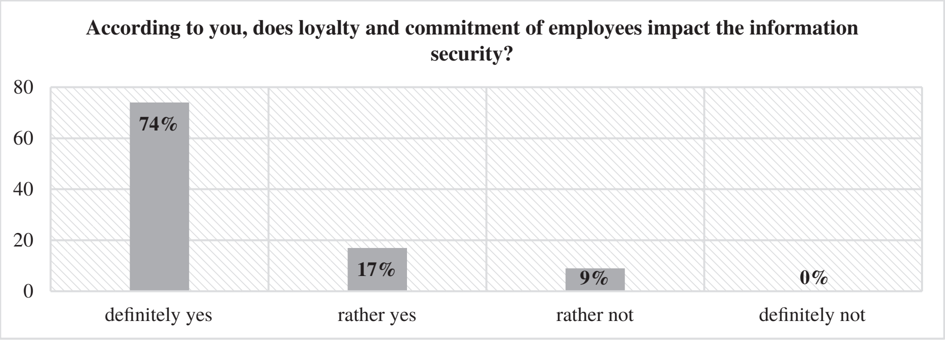


Figure 6. Elements of the organisational culture affecting the information security

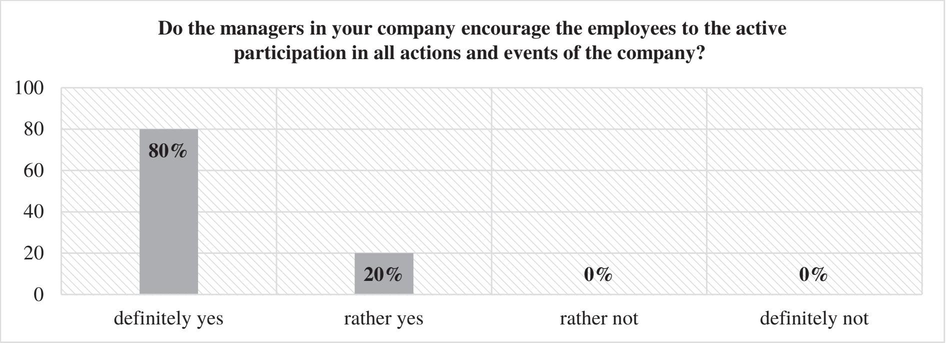
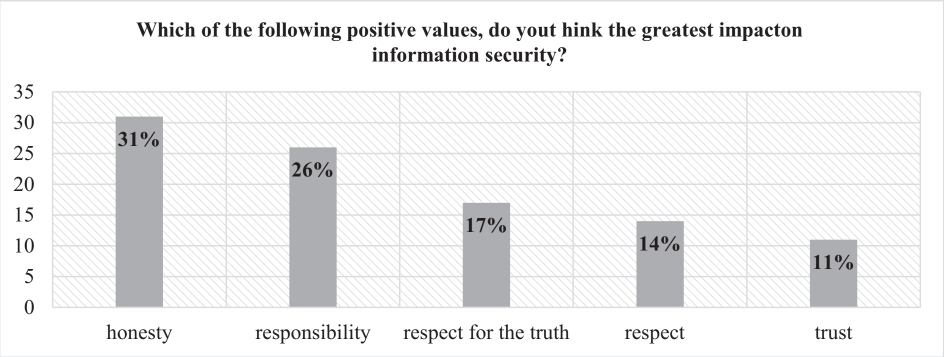


Figure 7. The actions of managers in the company

Figure 8.
The positive values, which impact the information security in the company



The data presented in Figure 5 show that the studied company is dominated by the positive organisational culture, characterised by openness, pro-activity and creativity of employees, what is confirmed by 49% of the respondents.

When considering the impact of elements of the organisational culture on the information security, the respondents were asked a question, According to you, does loyalty and commitment of the employees impact the information security? From the obtained data, which were presented in Figure 6, we can conclude that loyalty and commitment of the employees have a significant impact on the information security in the company. The dedicated and loyal employees largely pay attention to the observance of all procedures and guidelines of the information security policy.

The information security system is also significantly affected by the attitude of the managers, that's why in the survey there was asked a question: Do managers encourage the employees to the active participation in all actions and events of the company? The results presented in Figure 7, confirm that mangers in the studied company take an active part in engaging employees in various types of the company activities. Information security management in the company requires the cooperation of many factors, including in particular the appropriate attitude of the managerial behaviour, who supervise the information security process.

The last question referred to the positive values of the organisational culture, which affect the information security in the studied company. According to the respondents honesty (31%) and responsibility (26%) have the greatest impact on the information security.

The results obtained from two stages allowed to illustrate the state of the information security in the studied company, the level of information security management, the level of employee awareness in terms of the information security, but also to emerge a positive aspect of the whole information security management system, which mainly refers to the organisational culture prevailing in the company.

Positive values not only affect the improvement of the information security in the company, but also the better working atmosphere.

4. Conclusion

Information, regardless of how it is processed, is a valuable source of each organisation. That's why in recent times its importance is so significant, especially when the attacks of hackers are becoming more common. The information security system for many years has referred only to the technical aspect of security, avoiding the behavioural aspect. Numerous reports in the field of information security increasingly emphasise that the employees are the main source of the attack. Therefore, it is so important for the proper and effective implementation of the information security management system in the company to show the positive values of the organisational culture, the appropriate technological protection, as well as the supporting approach of the management towards the information security. The combination of these three aspects enables the efficient information security management in the company. The information security goals of employees should consistently be compared with the information security goals of management, expressed in the information security policy, to identify discrepancies (Thomson and van Niekerk, 2012).

The conducted study has contributed to the better understanding of the essence of the information security, as well as relations between the positive values of the organisational culture and the effectiveness and efficiency of the information security management system in the company.

The survey is only the basis for further extensive research on the behavioural determinants of information security management in the company.

References

Barczak, A., Sydoruk, T. (2003), *Bezpieczeństwo systemów informatycznych zarządzania*, BELLONA, Warszawa.

Chang, S. E., Lin, Ch. S. (2007), "Exloring organizational culture for information security management", *Industrial Management & Date Systems*, Vol. 107 No. 3, pp. 438–458.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp. 90–101. DOI: http://dx.doi.org/10.1016/j.cose.2012.09.010

Da Veiga, A., Martins, N. (2015), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", *Computers & Security*, Vol. 49, pp.162–176.

Eloff, J., Eloff, M. (2003), "Information Security Management – A New Paradigm", *Proceedings of SAICSIT 2003*, pp. 130–136.

Glińska-Neweś, A. (2010), "Pozytywna kultura organizacyjna jako pożądany efekt pozytywnego potencjału organizacji", in: Stankiewicz, M. J. (Ed.), *Pozytywny Potencjał Organizacji. Wstęp do użytecznej teorii zarządzania*, Wydawnictwo Dom Organizatora, Toruń, pp. 75–101.

Janczak, J., Nowak, A. (2013), *Bezpieczeństwo informacji. Wybrane problem*, AON, Warszawa.

Johnson, M. E., Goetz, E. (2007), "Embedding Information Seciurity into the Organization", IEEE *Security & Provacy*, Vol. 5 No. 3, pp. 16–24.

Korzeniowski, L. F. (2008), *Securikologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, EAS, Kraków.

Koskosas, I., Kakoulidis, K., Siomos, Ch. (2011), "Information Security: Corporate Culture and Organizational Commitment", *International Journal of Humanities and Social Science*, Vol. 1 No. 3, pp. 192–195.

Łuczak, J. (2009), "Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001", *Zeszyty Naukowe Akademii Morskiej w Szczecinie,* Vol. 19 No. 91, pp. 63–70.

Molski, M., Opala, S. (2002), *Elementarz bezpieczeństwa systemów informatycznych*, Mikom, Warszawa.

Ruighaver, A. B., Maynard, S. B., Chang, S. (2007), "Organizational security culture: Extending the end-user perspective", *Computers & Security*, Vol. 26, pp. 56–62.

Thomson, K. L. (2006), "Cultivating an organizational information security culture", *Computere Fraund & Seciruty*, Vol. 1 No. 10, pp. 7–11.

Thomson, K., van Niekerk, J. (2012), "Combating Information Security Apathy by Encouraging Prosocial Organisational Behaviour", *Information Management & Computer Security*, Vol. 20 No. 1, pp. 39–46.

Strebe, M. (2005), *Podstawy bezpieczeństwa sieci*, Mikom, Warszawa.

Stabryła, A., Woźniak, K. (red.) (2012), *Determinanty potencjału rozwoju organizacji*, Mfiles.pl Encyklopedia Zarządzania, Kraków.

Szczęsny, M. (2012), "Co nowego w zarządzaniu bezpieczeństwem informacji? Standard ISO 27001", *Zeszyty Naukowe Warszaswskiej Wyższej Szkoły Informatyki*, No. 7, pp. 95–108.

Urbanek, G. (2011), *Kompetencje a wartość przedsiębiorstwa: Zasoby niematerialne w nowej gospodarce*, Oficyna a Wolters Kluwer business, Warszawa.

Wołowski, F., Zawiła-Niedźwiedzki, J. (2012), *Bezpieczeństwo systemów informatycznych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*, edu-Libri, Kraków.

Wrzosek, M., Nowak, A. (2009), *Identyfikacja zagrożeń determinujących zmiany w systemie bezpieczeństwa społeczeństwa informacyjnego*, AON, Warszawa.

Zbierowski, P. (2012), *Orientacja pozytywna organizacji wysokiej efektywności*, Oficyna a Wolters Kulwer business, Warszawa.