J. Basic. Appl. Sci. Res., 3(8)520-524, 2013
© 2013, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Identifying the Determining Factors of Information Security Management System in Large Companies

Gholam Reza Memarzadeh[1], Samane Fayez[2], Pirhossein Koolivand[3]

[1]Faculty member of Science and Research University, Islamic Azad University, Tehran
[2]MA in Public Administration, Science and Research University, Islamic Azad University, Tehran
[3]Deputy of Development & Human Resource Development of Shafa' (Healing) Neuroscience Research Center

ABSTRACT

The purpose of this study is to identify the determining factors of information security management system in large companies. For this purpose, 130 staff of office of information technology of these companies were selected by using cluster random sampling method and responded to the self-made questionnaire of the research. The obtained data from the questionnaire were analyzed with the use of One- Sample t -test and the results indicated that internal factors including input, process and output factors and external factors including five factors of managerial, human, physical, cultural, organizational and security have significant effect (P<<0.01) on information security management system in large companies.

KEYWORDS: Security management, information systems, information security management system, large companies.

1. INTRODUCTION

Information is one of the most important assets of every organization and due to high value and its necessity for each organization, it should be protected in a good way. Some authors have assimilated information to blood in an organization veins which is considered as the resuscitative factor of organizations (Holliday et al., 1996; Von Solms& Vin Solms, 2006) and in case of limitations or endangering this flow, the organization will face death (Fulford& Doherty, 2003).

Information is often applicable for directing the staff processes from high levels to operational levels (Von Solms&Vin Solms, 2006). Decision making is a very important process in each organization and its basic is information processing which should have three characteristics of: confidentiality, correctness and availability otherwise it will bear a huge loss for the organization (Posthumus and Von Solms, 2004). Hence for proper use of the information of an organization and applying it in line with the organization's aims, we should protect them against any kind of loss and change. Further information is the connecting agent of other resources of an organization (Eloff et al., 1993). The importance of the role of business information of few recent decades of today's organizations is so much that so many of prominent researchers have noted its effects on different organizational dimensions as information revolution (Drucker, 1988). Therefore we should be sensitive toward the risks relevant to information and should identify and manage them (Posthumus and Von Solms, 2004). Hence for proper use of valuable information of an organization and applying them in line with the targets of the organizations should protect them against any kind of loss, change and/or deliberate or accidental distribution (Flowerday& Von Solms, 2005).

The security of information exchange space is one of the key business concerns during past two decades. This topic is one of the persistent problems and one of the most basic challenges of information technology managers and more importantly the security of information exchange space have changed into one of the most important issues during recent years in the field of information technology (Gonsalves, 2005).

In spite of availability of advances technologies in the field of security of information exchange space, the number and intensity of attacks is increasing and there is no sign of decrease in it (Cisco, 2007).

The main purpose of implementation of a security information system is protection against unauthorized access, providing information accessibility to authorized users, protecting information against breaching that threaten its health and detection of security breaches. Also, due to the novelty of the information security field, it seems that the topic of information security management system has not got much of attention and in practice only a few researches have been conducted in this field (Gordon, 2002) and the researches' results indicate that the market of the security of information exchange space does not have a proper performance and so many organizations do not allocate much budget on their information security because its cost is so high. On the other hand, the costs of not

***Corresponding Author:** Gholam Reza Memarzadeh, Faculty member ofScience and Research University, Islamic Azad University, Tehran. Email: g.memar@gmail.com

having it such as network's failure and customers' worries, which are not lasting, is low. Further, the costs of tendency and transition to a new technology which has a higher security is often high and this causes the managers of an organization to think less of turning to a new technology. The combination of the above mentioned factors, i.e. asymmetry of information, the high cost of obtaining information regarding security points of products and high cost of transition to a new technology causes people and financial organizations, etc not to invest so much in the management of the security information systems which in turn can have adverse effects.

Due to the importance of this topic, unfortunately, enough attention has not been given to information security in Iranyest and no organization in Iran has succeeded in obtaining required and necessary standards for information security and no research has been conducted which would identify the determining factors of information security management systems in large companies.

It should be noted that, due to the expressed opinions in this field, it can be claimed that creating information security management system in all organizations is vital and necessary, especially in public organizations. Creation and development of this system, in line with development and extension of application of information technology in ministries, institution and organizations, will lead the country to enter information society in a more prepared manner.

In spite of the significance of information security and the effect it has had in the success and advancement of most countries, this issue has not studied in a proper manner in Iran and this can be considered as a good opportunity. Hence, considering the above- mentioned issues, this paper is seeking to study the pathology of Information Security Management System in large companies.

Regarding the studies done in this area, Mitchell et al. (1999), in their study, have focused on human tendencies regarding information security among key decision makers in commercial organization of England. They found out that the security of the information of a company has a great deal of importance for guaranteeing the business survival of it. Many organizations do not take information security management seriously which makes them vulnerable toward risks and the main reasons include the following:

- Limited awareness exists regarding information security threats.
- Intensity of management and awareness from information security is only high in IT department.
- Electronic information is seen as an intangible asset.
- Potential security risks resulting from internet access have not been fullymet and most of the companies have not yet faced a security problem or issue.

Therefore, they are not ready to participate in security actions. It was suggested that companies should consider the following recommendations for preventing misuse or losing information assets:

- All the possible security threats and quantity estimation of potential costs should be based on a formal risk analysis.
- Information security management from an IT-based operation should be released.
- Encouraging this perspective that information is a valuable company asset.

Bjorck (2001) has described experiences and perspectives according to important vital factors for implementation processes and certificate issuance. Empirical aspect of his studies is focused on the experiences and perspectives of certificate issuance inspectors as well as security information consultants for implementation and certificate issuance of information security management system. These factors include the following:

1. Management commitment: this factor has received the most attentions from the inspector respondent group.
2. Well-structured project: this factor was introduced by respondents who have reminded the important role of structure in risk analysis and organizational responsibilities.
3. Holistic approach: respondents emphasize on the ability of the project members as well as other staff in observing the complete image of business issue, which gives them the ability to achieve a complete view of the economical agency. This factor is combined with information security process as well as the organization process so that the information security management system may not stop at security or IT department.
4. Valuing the information security necessity: this factor was mentioned repeatedly by respondents and proved the necessity of information security for the whole organization. This item should be extended for covering all the aspects of information systems.
5. Motivated staff: most of the responses are focused on motivation of the individuals participating in information security management system project such as project participants, project manager and those responsible in different fields of an organization.
6. Access to external capabilities: ability of calling up external capabilities at the time of necessity is an important factor which proves the need of professionals and consultants of IT and information security.

The other six factors were defined by considering the implementation consultants of information security management system regarding implementation and certificate issuance of information security management system.

1. Project management capability: refers to an effective capability of project management for successful implementation of basic information security management system such as the need of active members for project, a proper organization for the project and a reasonable timetable.
2. Commanding capability: this capability strengthens the role of top management with defining and supporting information security through awareness and participation of management in information security.
3. Financial capability: determining the required resources for actual estimation of costs.
4. Analysis capability: this aspect emphasizes on the importance of analysis ability for strengthening the information security management system through reasonable balanced policy.
5. Communicating ability: the interaction process between information security management and other sections is an important factor and the efforts toward information security should not stop the desk of security management.
6. Implementation ability: development of information security policy is an important issue which includes all regulations, opinions, controls and security procedures. It is necessary that these policies will be implemented and practiced. In addition, staff should be influential on IT ideas and other departments of the organization.

In general, the basic successful factors in theoretical studies have been introduced. Some of these factors have been examined and proved in empirical studies while some of them have not been tested yet.

From theoretical point of view, the 2nd generation of information security management system has defined multiple evaluation programs and most of the organizations like to share their information based on programs like these (Von Solms, 1999).

Von Solms (1998) has introduced the hypothetical frame of information security management system to observe how information security management system is adopted in the field of risk management. Kwok & Longley (1999) have defined the data storage model risk which is used to accelerate the process of risk analysis through specifying the external effects on operational systems. Eloff&Eloff (2003) have described information security management system as a process which is focused on planning and implementing practical management and on the other hand have described implementation of information security management system as organizations ability to evaluate software productions.

All of these patterns and theories prove the importance of implementation of information security management system. Therefore, we need multiple factors for successful implementation of information security management system and forgetting these factors will put the information assets at high risk. Strengthening preventive measures, developing security solutions and implementation of corrective actions for increasing the users' knowledge of these factors are more trustable from success point of view. Love (2007) and Mitchell et al. (1999) empirically, have focused on importance of information security for the same business continuity. They have specified the reasons which possibly cause the companies not to be ready for security events.

METHODOLOGY

The current research is an applied research from the aim point of view, descriptive-correlative from method point of view, and survey research from the point of view of conduct manner.

Research population and sample

The population of the current research includes managers and professionals ofthe office of information technology of large companies of Tehran. For determining the required sample for our research, the cluster random sampling method was used in this way that the researcher has first divided Tehran into five regions of North, South, Center, West and Eastgeographically and then based on 22 districts of Tehran. Then, each district has randomly selected one area and from each selected area, the managers and professionals related to information security in the office of information technology of large companies of Tehran were selected. Finally, a total number of 130 managers and experts were selected for main study.

Instrument

In the current research, for identifying the determining factors (or key factors) of information security management system in large companies, we used the researcher-made questionnaire, having items regarding the most important determining factors (or key factors) of information security management systems. Content validity of the questionnaire was confirmed by professionals and academics of this field and its reliability was calculated by Cronbach's alpha, which was equal to 0.82,indicating the proper reliability of the questionnaire.

Research findings

In this research, in order to study the determining factors of information security management system in large companies, an independent-sample t-test was used. Table 1 indicates the results.

Table 1. Results of independent sample t-test

T criteria = 3					
Variable	**Mean**	**Standard deviation**	**df.**	**t**	**Sig.**
Input factors	3.18	0.69	129	3.048	.00
Process factors	3.40	0.70	129	4.466	.00
Output factors	3.81	0.64	129	14.568	.00
Managerial factors	3.65	0.74	129	9.937	.00
Humane factors	3.42	0.62	129	7.730	.00
Physical factors	3.48	0.70	129	7.767	.00
Cultural factors	3.41	0.74	129	6.230	.00
Organizational factors	3.34	0.78	129	4.954	.00
Security factors	4.08	0.45	129	27.360	.00

As it is clear from the above tables, from the point of view of managers and professionals of the office of information technology of large companies in Tehran, input, output, process, managerial, humane, physical, cultural, organizational and security factors have a significant effect ($p<0.01$) on information security management system.

CONCLUSION

Todays, with the advancement of information technology in human life and more dependence of them on business, protection of information is considered as the most vital vein of a modern industry. Information is one of the most valuable and sensitive assets of an organization. Obtaining information and providing the required information timely and properly have always had a central and decisive role. Maintaining information is the required condition for continuity the business process of economical agencies. Unauthorized access and breaching the information on disks, computers and its unauthorized use has turned into problem. These accesses are done by the employees of an organization, internet users or by other agents. Hence, organizations and companies have to seek to implement security programs. For implementing these security programs, only focusing on technical matters is not enough but also we need to control the policies and correct procedures and, at the same time, we need to standardize them to increase the percentage of information security and this is the reason that companies are required to apply information security management systems (Bohrani and Yazdi, 2009).

The security of the information exchange space has such characteristics which puts it under the category of public goods with external effects. It is necessary to note that lack of security in a system will have negative effect on other systems. Lack of security in internet and computer is like air pollution. In fact, using one vulnerable system creates external negative effects because this system will turn into a place for viruses and worm's attacks and eventually will lead to the failure of network, etc. In this situation, users will not bear the complete cost resulting from the actions and will make other people to bear the costs also.

In conclusion, nowadays, for considering national modern economies, which are completely dependent on information technology for their survival, our need to security of information and information systems is inevitable. The current paper has tried to study the determining factors (or key factors) of information security management system in large companies. The results of inferential data analysis indicated that, from the point of view of managers and professionals of the office of information technology of large companies in Tehran, input, process, output, managerial, humane, physical, cultural, organization and security factors have significant effect ($p<0.01$) on information security management system.

In the current world, the need to protect information has become more than the past (Knapp et al., 2006). Also, the amount of electronic information has become more and technology is continuously being changed and as a result we should understand the disadvantages of information and consider them in electronic systems (Wolf-Wilson and Wolfe, 2003). In recent years, some believe that information security is not a technical issue any more but it has turned into a managerial issue (Entrust, 2004; Posthumus and Von Solms, 2004) and all of them has focused more on the necessity of application of intelligent approaches for increasing the security of information systems.

REFERENCES

1. Bjorck, F., 2001.Security Scandinavian style, Master's thesis, Stockholm University &Royallnstitue of Technology.
2. Bohrani, P., and M. Yazdi, 2009. Importance and necessity of information security management system in electronic government. 2nd international conference of electronic administration systems.
3. Booysen H, Eloff, J, 1995. A methodology for the development of secure application systems, In: Boft J-1P, von fulms s-i, editors. Information security - the next decade.IFIP, Chapman & Hall. ASSDM;. p. 255-69.
4. Cisco, A, 2007.Annual Security Report.
5. Doherty, Neil F., Fulford, H., 2006. Aligning the information security policy with the strategic information systems plan. *Computers and Security*, 25: 55 - 63.
6. Drucker, P. F., 1988. The coming of the new organization, *Harvard Business view*, Jan-Feb.
7. Eloff, J. and E. Mariki, 2003.Information security management: A new paradigm. *ACM*, 130-136.
8. Eloff, J.H.P., Labuschagne, L., Badenhorst, K.P., 1993. A comparative framework for risk analysis methods.*Computers and Security*, 12(6):597-603.
9. Flowerday, S., Von Solms, R. 2005.Real-time information integrity, system integrity data, integrity continuous assurances.*Computers & Security*, 24: 604- 613.
10. Gonsalves, D., 2005. Parallelization of the swat watershed model for application on the supercomputers at the Hawaii supercomputer center.
11. Gordon, M. 2002. When should companies go public following a security breach.*Computer Fraud & Security*, 16-19.
12. Halliday, S,Badenhorst, K, Von Solms, R.,1996. A business approach to effective information technology risk analysis and management. *Information Management and Computer Security*, 4(1):19-31.
13. J, Knapp Thomas, E, Marshall, R, Riner, K, Nelson Ford, F. 2006. Information security: Management's effect on culture and policy. *Information Management & Computer Security*, 14(1):24-36.
14. Kwok, L., Dennis, L., 1999. Information security management and modeling information, *Management & Computer Security*, 30- 39.
15. Lau, O., 2007. The ten commandments of security.*Computer & security*, 17:1191-2380.
16. Mitchell Ruth C., Marcella, R., and Baxter.C, 1999.Corporate Information Security Management. *New Library World*, 213-227.
17. Posthumus, S., Von Solms, R., 2004.A framework for the governance of information security.*Computers & Security*, 23, 638-646.
18. Von Solms, R., 1998. Information security management (2): guidelines to the management of information technology security (G\IIITS). *Information Management & Computer Security*, 6/5:221-223.
19. Von Solms, R., 1999. Information security management: Why standards are Important.*Information Management & Computer Security*, 7/1: 50-57.
20. Von solms, R., Von Solms, S.H., 2006.Information security governance: Due care.*Computers & security*, 25: 494 - 497.
21. Wolfe-Wilson, J., and Henry, B. 2003.Management strategies for implementing forensic security measures. *Information Security Technical Support*. 8(20): 55-64.