Research Journal of Management Reviews. Vol., 3 (1), 8-12, 2017
Available online at http://www.rjmrjournal.com
ISSN 2149-9168 ©2017

Identification of the Factors Associated with Strategic Decision-Making Information Security in Airports in Golestan Province

Mohammadreza Enayati Shabkolaee, Ahmad Mehrabian*

Department of Management, Aliaba Katoul Branch, Islamic Azad University, Aliaba Katoul, Iran

*Corresponding Author Email: mehrabian.project@gmail.com

Abstract: The purpose of the research was to identify the factors associated with strategic decision-making information security in airports in Golestan Province. The research method was descriptive-survey and the present study sample was directors and deputies of different parts of airports in Golestan province for 30 people. Articles, books and experts were listed in the implementation of criteria and sub-criteria research related to strategic decision making information security in airports in Golestan Province and after filling the questionnaire of the identification, major and minor criteria were identified. According to data analysis, three criteria of environmental factors, structural factors and management factors (15 sub-criteria) were identified as the factors associated with strategic decision-making information security in airports in Golestan Province.

Keywords: Strategic Decision-Making, Information Security, Airports in Golestan Province.

Introduction

Strategic information systems planning include the element of strategic thinking the most desirable information systems are identified and designed for the company so that long-term activities and policies of IT and the macro-policies of the organization can be integrated with each other. In other words, strategic information system planning is a mechanism for assurance because IT activities step on the scope of the organization and its strategies (Sebherwal & Chau, 2012). Information systems strategic planning is a process in which a set of computer-based capabilities is identified and implemented in the organization. This planning must be supported from programs and organizational goals to win them over. In other words, information systems strategic planning is a strategic thinking process that information systems of the organization are identified to favorable followings so that the organization can implement long-term goals and policies (Newkirk et al., 2008).

Alignment is a key component of success for strategic information systems planning which coordinates the relationship between information systems strategy and business strategy. Strategic information systems planning success would be possible if there was an alignment between these systems, goals and business strategy. In other words, this alignment should be considered in planning. The alignment of technology activities and organizational strategies is examined in this dimension (Hosseini et al., 2013). Today, conditions and competitive environment of the organizations have been more complex, varied and widespread than before and the managers deal with a variety

of decision-making. Many methods have been proposed for making management decisions that the aim of all of them is to achieve an optimal decision, but what is more important is the decision-making methods and tools, strategic decision-making information security. It seems that different organizations with regard to the importance of the information contained in them require strong management in order to maintain the security of this information (Syamsuddin, 2011). Information security points to protect data and minimize unauthorized access. The concept of Information Security Management System includes: the security of information for some of the overall information security management system in an organization based on business risk approach and the aim is to establish, implement, operate, monitor, verify, maintain and improve information security (Anderson, 2010). Organizations and companies including airports, according to the importance and value of their information require the design of a robust Information Security Management System that they should update their system along with environmental changes so that they can provide advances in technology, access to data for different organizations easily (Moqaddasi & Ayani, 2013).

Information systems in centers of the airports play a supporting role for providing the services. Large amount of information on each organization in the form of drawings, plans, policies, circulars, business correspondence, documentation and research projects and other information which we put this technology to store and process it in, we are forced to think about protecting it picks up too. These data are the most important asset and the key to growth and success of any organization. If we cannot maintain this important asset of the reach of strangers and other threats, we will see the severity of injuries (Mahmoudzadeh & Radrajabi, 2006). Information Security Management is a part of the management information which has a responsibility of determining the aims of the security and investigating the security objectives and obstacles to achieving these goals and providing the necessary solutions. Also, the management of the security has the duty of implementing and controlling the system performance of the organization system and finally, it should attempt to update the system.

The purpose of the management of information security in an organization is to keep assets (software, hardware, information and communication and human resources) organizations against any threat (including unauthorized access to information, environmental risks and hazards created by system users). Therefore, the purpose of the research was to identify the factors associated with strategic decision-making information security in airports in Golestan Province.

Materials and Methods

The research method was descriptive-survey and the present study sample was directors and deputies of different parts of airports in Golestan province for 30 people that all of them were selected as a sample. In the stage of performing the study, after providing a preliminary explanation about measurement instrument and the purpose of the test, how to answer test for participants were described in detail. On the ethical considerations after obtaining the consent of the people and giving necessary awareness, they were assured that information received will be used only to this study and they will be protected from any abuse. Two semi-structured questionnaire were used to measure the variables. First, the opinion of the experts is listed to identify the factors associated with strategic decision-making information security in airports in Golestan Province and they were categorized in both the criteria and sub-criterion and in the second phase, the experts allocated to the criteria and sub-criterion using standard AHP paired comparison questionnaires and their ratings were considered to calculate. The analysis of AHP hierarchy was used to analyze the data.

Results

First, according to the review of texts and previous research done and the use of the viewpoints of different sector managers and deputies in airports in Golestan Province, hierarchical decision structure should be designed in order to identify the factors associated with strategic decision-making information security that 3 main criteria and 15 sub-criteria are categorized due to the outcome of this stage. First, a set of sub-criteria was identified through a questionnaire survey shown in Table 1 for 3 main criteria. The method was that among the sub-criteria which were selected for each main criterion and regulated in the questionnaire A and completed by deputies of different sections in airports in Golestan Province, the sub-criteria which an average intensity of the impact were from 0 to 2 were used to set the next questionnaires (rating questionnaire of strategic decision-making the factors related to information security) and the sub-criteria which an average intensity of the impact were from 0 to -2 were omitted. The questionnaire A by the team of decision making was answered containing 30 people of directors and deputies of

different parts of Golestan province airports. According to the following Tables, it has been discussed on what was mentioned closely.

Table 1. A summary of information related to the sub-criteria of management factors.

Criterion	Sub-criteria	The mean of the severity of the impact	Max	Min
Management factors	Lack of time of management and project financing	1.95	2	0
	Taking advantage of the full support and participation of senior management	1.26	2	0
	Senior management awareness of the need for information security management	1.21	2	0
	Having sufficient expertise and experience of senior management	1.65	2	0
	Appropriate development of information security policy	1.32	2	0

According to Table 1, this is regulated to measure the severity of the impact of the main criterion in the factors related to strategic decision making information security according to the survey of the responses obtained. As it can be seen, an average intensity of the impact and average maximum and minimum intensity of the impact of the sub-criteria of the management factors has been accepted. According to Table 2, all 7 sub-criteria were accepted by the management factors.

Table 2. A summary of information related to the sub-criteria of structural factors.

Criterion	Sub-criteria	The mean of the severity of the impact	Max	Min
Structural factors	Coordinating organizational structure to the needs of information security management system	1.303	2	0
	Organizational maturity	1.29	2	0
	Having a good governance committee	1.42	2	0
	The stability of senior management	1.67	2	0
	Having the organization to re-engineering of the processes	1.56	2	0

According to Table 2, this is regulated to measure the severity of the impact of the main criterion 2 in the factors related to strategic decision making information security according to the survey of the responses obtained. As it can be seen, an average intensity of the impact and maximum and minimum intensity of the impact of the sub-criteria of the structural factors has been accepted. According to Table 2, all sub-criteria were accepted by the structural factors.

Table 3. A summary of information related to the sub-criteria of environmental factors.

Criterion	Sub-criteria	The mean of the severity of the impact	Max	Min
Environmental factors	The attention to information security management system as a competitive advantage	1.33	2	0
	Parallel institutions in decision-making (Information Technology and Security)	1.23	2	0
	Holding training courses	1.64	2	0
	Cooperation and coordination staff involved with the project	1.39	2	0
	Enjoying the consultant externally	1.29	2	0

According to Table 3, this is regulated to measure the severity of the impact of the main criterion 3 in the factors related to strategic decision making information security according to the survey of the responses obtained. As it can be seen, an average intensity of the impact and maximum and minimum intensity of the impact of the sub-criteria of the environmental factors has been obtained and an average intensity of the impact has been accepted obtaining from 0 to 2. According to Table 3, five sub-criteria were accepted by the environmental factors.

Discussion and Conclusion

The purpose of the research was to identify the factors associated with strategic decision-making information security in airports in Golestan Province. In order to achieve this goal, based on the literature related, the strategic decision-making factors related to information security in airports in Golestan province with 3 main criteria and 15 sub-criteria were identified and designed. According to data analysis, three criteria of environmental factors, structural factors and management factors (15 sub-criteria) were identified as the factors associated with strategic decision-making information security in airports in Golestan Province. Similar research has been done in the past. For example, Tajfar et al (2014) in a research discussed on investigating ranking the barriers to implementing information security management system and assessing the preparedness of the exploration management. Today, information plays a capital role of an organization and data protection of the organization is one of the most important pillars of its survival. Information Security Management System defines the protection of information in three specific concepts of data confidentiality, integrity and availability of information.

Many failures to implement information security management system root in organizational matters and given the state of readiness of the organization before implementation. In this research, it has been attempted that the barriers to implementation of information security management system in terms of importance are rated in the Analytic Hierarchy Process and the organization's readiness to implement information security management system is determined to help determine the questionnaire. The results consider the discrepancy of the organizational structure to the needs of information security management system as the most important obstacle to the implementation of information security management system and staff fear of hard work processes by implementing security management system has introduced information as the least significant obstacle while the readiness of exploration management in the implementation of information security management system is lower than the average limit. Generally, the staff focuses on the tasks and job descriptions in the organizations and information security is less of a target. In today's world, information is considered the most important organizational asset and the protection through information management systems is necessary.

The main objective of this study is to identify models of information systems security management in an organization and evaluate the effect of the factors that these systems are faced with the risk of theft and changing information. To this end, international standard models coordinated with the structure of organizations in Iran were selected and they were used in three levels of knowledge, attitude and behavior in the development of theoretical framework along with the awareness of the security of user data. Finally, some suggestions were presented and emphasized for the establishment of the cycle of information security in the organizations that they were more emphasized to maintain the security of information, in addition to technical solutions to non-technical and human factors such as promoting the awareness of employees and managers. Moqaddasi and Ayani (2013) discussed on studying data security in health information systems in a research. Health care organizations are producing health data in the context of information systems. Preserving the original nature and the nature of the data in a secure environment to provide good service and quality to patients are some tasks for information system. The evaluation of features of health data requiring necessary the need to secure the data and also introducing the attempts performed to create a data security standards in information systems are the purpose of this study.

The findings of this study on the importance of health data suggest that three factors which they are considered the reasons for the need for data security in the health field include confidentiality, the risk of financial abuse, biomedicine and behavioral sciences. On the other hand, given the importance of health data and the necessity of their securing, most organizations have attempted on national and international standards such as: *ASTM ،CPRI ، AAMC ،NAIC، ISO 27000 and HIPPA*. It is noteworthy that the emergence of new and different discoveries can lead to production of a new health data; therefore, identification of health data and their properties in order to select an appropriate security strategy are an important step in effective designing health information systems. As with all studies, this study has also some limitations. One of the problems of implementing hierarchical techniques is to understand the questionnaires. According to the previous experiences of the author, the questionnaires that have acceptable consistency are very difficult and in some cases, the questionnaire should be returned several times to

obtain a questionnaire which has the reasonable adjustment. Therefore, it was tried that most research questionnaires be received in person so that in cases where the questionnaires was incomprehensible for the managers, details should be given and in some cases, the questionnaires were returned several times.

Conflict of Interest

The authors declare no conflict of interest.

References

Anderson, R. (2010). Why Information Security is Hard: An Economic Perspective. Proc. of 17th Annual Computer Security Applications Conference, 10-14.

Hosseini, S. Y., Yousefi D., & Eskandari, A. (2013). The factors affecting the success of strategic information systems planning, Journal of Information Processing and Management, 29(1), 63-88.

Mahmoudzadeh, E., & Radrajabi, M. (2006). Security management in information systems, management science of Iran, 4, 78-112.

Moqaddasi, H., & Ayani, S. (2013). Data security in health information systems, Journal of security protection research of University of Imam Hussein (PBUH), 2, 127-137.

Newkirk, H. E., Lederer, A. L., & Johnson, A. M. (2008). Rapid business and IT change: drivers for strategic information systems planning?. European Journal of Information Systems, 17 (3), 198-218.

Sebherwal, R., & Chau, Y. E. (2012). Alignment between business and IS strategies A study of prospectors, analysers and defendes. Information System Research, 12 (1), 11-33.

Syamsuddin, I. (2011) Strategic Information Security Decision Making With Analytic Hierarchy Process, International Research Journal of Applied and Basic Sciences. 2 (11), 426-432.

Tajfar, A. H., Mahmoudi, M., & Soltani, R. (2014). Ranking the barriers to implementing information security management system and assessing the preparedness of the exploration management, 6(4), 551-566.