Risk assessment of Information Security Management System inGovernment Organizations in Iran

Samane Fayez[1] ,HodaHosseinZade Nazeri[2] , Mohammad BagherKiaroodi [3]

[1]Department of public administration, Islamic azad university, science & research branch, Tehran , Iran
[2]HUBS (Huddersfield Business School) Huddersfield university, UK
[3]Department of Information Technology Management, Islamic azad university, science & research branch, Tehran , Iran
Samane.fayez@yahoo.com, Hodahosseinzadenazeri@yahoo.com, m.kiaroodi@gmail.com

Objective: The main objective of this research was to study the risks involved in information security management systems (ISMS) in large corporations.

Methodology: Data was collected by a researcher made questionnaire. The reliability of this questionnaire was examined by Cronbach's alpha measured at 0.86. The validity of questionnaire was confirmed by experts in this field. This confirmation proved the face validity and content validity of the questionnaire. Pearson correlation coefficient and two variable regression analysis was used for data analysis.

Findings: The findings showed that and risk reduction of ISMS has significant relation with security management system department, human resource development, security management system training, strategies and policies for information security, risk assessment of information processing security, security incident support in large organizations.

Conclusions: the important role of information in today's business and the requirement for safeguarding corporate information make it necessary for every organization to undertake the task of designing ISMS that fits its information base in order to safeguard the corporate information assets.

Keywords: Management System, Information Security, Large Corporations

1. Introduction

The expansion of computer network and the availability of varied computer hardware, software packages, and network complexity have increased the risk and vulnerability of organizational information systems. Security risks and system vulnerability has increased the opportunities for embezzlers and hackers to make unauthorized access to corporate information and abuse their database. The security risk is now at a level that a mere installation of firewall or router will not provide sufficient protection to information systems. Information security is vital to the expanding information technology with widespread impact on individuals and organizations. Information security and maintenance have significant role in organizational business and activities.

An important issue in information security management is its integration into business processes instead of considering it as a separate supporting entity. Security tasks and management should be considered as one of daily responsibilities (Posthumus&Solms, 2004). Information security strategies should be integrated in overall corporate strategies. Corporate ISMS should become one of the main business processes (von Solms& von Solms, 2006).

Government organizations and large corporations need ISMS. Information security has not attracted enough attention in spite of its importance and impact on success and growth of organizations. This could open opportunities for practitioners of this field. This study was conducted to assess the risks that should be considered for ISMS in large organizations.

2. Methodology

There are many research methodologies currently in use. The use of any one methodology depends on the nature of research and the variables under study. The research method in behavioral science is selected based on research objectives, data collection method, and the implementation approach (Bazargan et al, 2009). This study had practical objectives, used descriptive-survey method, and employed questionnaire for implementation.

3. Statistical Population and Sample

The statistical population in this study was one large corporation (with undisclosed name). This study attracted the assistance of 16 experts from the total population of experts in that organization for its data collection. The qualifications that were taken into account in selection of experts were as follows:

1. Education
2. Related experience in ISMS
3. Expertise in ISMS

Because of the limited number of experts in this company, all of them were included in this study. Therefore a census method was used for data collection

4. Research Tool

This study was a survey and used a researcher made questionnaire for data collection. This questionnaire included demographic questions plus 29 specialized questions related to risk assessment of ISMS in large organizations. The questions had five choices made on Likert scale from very low to very high. The reliability of the questionnaire was measure at 0.86 by Cronbach's alpha. This figure shows the high reliability of the questionnaire. Face and content validity of questionnaire was confirmed by the experts in this field.

5. Research Findings

The objective of this study was to assess the risks and

threats to ISMS of large corporations. One large corporation was selected and studied for this research.

** P<0/01 * P<0/05

Pearson correlation coefficient showed that risk reduction of ISMS in large corporations has significant relation with the following subscales.

1. Information security department in large corporation (p<0.01, r=0.81);
2. Publicity about the security system, human resource development, information security training (r=0.89, p<0.01);
1. Information security strategies and policies (r=0.51, p<0.05);
2. Risk assessment plan for information technology and security incident support (r=0.86, p<0.01); and
3. Written operational procedures and technical guidelines in large corporations (r=0.75, p<0.01).

Table 1 Correlation Coefficient of Research Variables

Variable	1	2	3	4	5	6
Information Security Facilities	1					
Human Resource Development	0.61 *	1				
Security Strategies and Policies	0.30	0.37	1			
Security Risk Assessment Plan	0.56 *	0.68 **	0.59 *	1		
Written Operational Procedures	0.75 **	0.52 *	0.08	0.54 **	1	
Risk Reduction of Information Security Management System	0.81 **	0.89 **	0.51 *	0.86 **	0.75 **	1

The high level of correlations is indicative of strong relation between variables. The direction of correlation shows that an increase in any variable will produce higher risk to ISMS, or vice versa.

Table 2 shows the result of two-variable liner regression analysis on the study variables.

Table 2 Effect of Variable Changes on Risk Reduction in Information Security Management System

Variable	R^2 adj.	Beta	F	P
Information Security Facilities	0.63	0.81	26.839	0.00
Human Resource Development	0.78	0.89	55.057	0.00
Security Strategies and Policies	0.21	0.51	5.040	0.04
Security Risk Assessment Plan	0.72	0.86	39.352	0.00
Written Operational Procedures	0.53	0.75	17.853	0.00

Data analysis performed on the study sample showed that 0.63 of risk reduction in ISMS could be determined by facilities provided by information security department at 0.01 level of confidence. The figures for other subscales were:

A. 0.78 for human resource development at 0.01 level of confidence;
B. 0.21 for security strategies and polices at 0.05 level of confidence;
C. 0.72 for security risk assessment plan at 0.01 level of confidence;
D. 0.53 for written operational procedures at 0.01 confidence level.

6. Discussion and Conclusions

Many organizations do not take information security management very seriously. This attitude increases their vulnerability toward potential risks. The reasons for lukewarm reception are (Khani, 2009):

- Limited awareness about the information security risks;
- Awareness level is only high in information technology department;
- Electronic information is viewed as non-tangible asset;
- Potential risks associated with internet access are not completely estimated; and
- Most companies have not faced a real security problem.

Military conflicts of decades ago have given way to all out confrontations that involve politics, economic, cultural, technology as well as military. This development forces countries to prepare for non-military defense against possible threats. Non-military defense refers to mechanisms that do not require military hardware. The purpose of building such mechanism is to prevent or minimize possible damages to critical and vital equipment, facilities and human resources.

The present information infrastructure of country is totally dependent on information technology. Information technology has increased the speed and quality of services. However, the widespread availability of information technology opens the information infrastructure to new potential risks.World is facing rapid and extraordinary changes in many areas in the push for globalization in the third millennium. These changes produce many opportunities and threats for organizations. Managers should take the necessary measures to take advantage of the opportunities and confront the possible threats. The required actions may involve structural, technical, or behavioral modification. Such undertaking will require risk assessment and phenomenology of the processes that face modifications (Raja'ee Pour, 2009).

Two supporting theorems in this study are system theory and open system theory. No danger could threaten the organization when a dynamic order prevails in ISMS. Open

system theory comes into play in risk assessment of a system (Katz & Kahn, 1978). Open system theory assumes an organization as a system with input, processes, and output. Feedback loops connect the three elements of a system and show the effects of input and output on its functioning.

Most of risk assessment models are made based on open system concept (Raja'ee Pour, 2009). Open system theorem assumes organizations as social systems that operate in their environment and take input from it (Katz & Kahn, 1978). Open system theory operates on input, processing, output, and re-input cycle.

Rapid move on the information highway has driven countries into information society with rapidly growing information systems and services. The majority of services are presently provided in such an environment. Therefore, service providers and users have no other choice other than joining the information society.

The information that once was kept on shelves and cabinets became available within the organization through its internal network. Information access could be controlled by putting limits on the number of users, limiting access types, limiting operation types, and other forms of access control. No serious security problem could occur on an internal network with these controls in place.

The situation changes drastically when an internal network is connected to the international network. Valuable organizational information could become accessible to various users all over the world. Such exposure puts corporate information at risk. Outside users are not the only potential threat. Studies have shown that the majority of threats to organizational information and information systems are originated within an organization by deliberate or unintentional acts of employees. This fact proves the need for ISMS to protect valuable corporate information assets.

The role of information in today's business operations and the requirements to safeguard it make it necessary for organizations to plan for ISMS suitable for their level of information processing. Safeguarding national information has been an issue for governments in the past. Access to sensitive military and national information by strangers has destroyed many nations throughout the history. Consequently, security in the information age has found new dimensions because of the importance of information as a business tool and as a profitable asset. Information security has become vital for company survival. Therefore, valuation and security of corporate information are critical for information system and members of organization.

Organizations do not presently invest enough in security systems. They do not exercise enough control over security risks and do not have sufficient safety measures in place to protect corporate information against possible threats. A national strategic plan for the security of information exchange underlines the importance of the issue. High Commission for Security of Information Exchange issued a directive to emphasize the need for a plan to implement measurements for security of information exchange in government organizations with a special recommendation for the design and implementation of ISMS. The publication of a guide for implementation of ISMS in 2004 made it mandatory to install such system based on current guidelines and standards.

Selection of ISMS is a strategic decision making. Design and implementation of ISMS should be based on organizational objectives, requirements, security needs, applied processes, and structure. The current security level of national information exchange environment is not acceptable, especially in government organizations. Many implemented information security management systems in large organizations have not been successful.

The need for information security prompted this study to examine the risk of ISMS in large organizations. The result of this study show that risk reduction in ISMS in large organizations has significant relation with publicity plan for information security, human resource development, security strategies and policies for information technology, risk assessment plan for information technology security, support for security violations events, documented operational procedures, and technical guidelines.

References

[1] A.Bazargan. "Research Methodologies in Behavioral Science", Agah Publishing, pp 101-202, April 2009.

[2] D. Katz &R.I.Khan." The social psychology of organizations", vol 8, pp.200-400, New York, 1978

[3] S. Posthumus&R.VonSolms," A framework for the governance of information security", Computers and Security, no 23, pp.638-646, March 2004.

[4] A. Khani."A Model of Effective Variables in Information Security Management Systems in Government Organizations", MA Thesis, Information Technology Management, pp.50-100, April 2009.

[5] R.VonSolm&S.H Von Solms." Information, Security Governance: A model based on the Direct- Control Cycle", Computers and Security, no 25, pp. 408-412, March 2006.