J. Basic. Appl. Sci. Res., 2(3)2582-2588, 2012
© 2012, TextRoad Publication
ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Information Security Management on performance of Information Systems Management

Shahram Gilaninia[1]; Seyyed Javad Mousavian[2]; Orang Taheri[3]; Hamid Nikzad[3]; Hoda Mousavi[3]; Fatemeh Zadbagher Seighalani[4]

[1] Associate professor, Department of Industrial Management, Rasht Branch, Islamic Azad University, Rasht, Iran
[2]Department of Management, Astara Branch, Islamic Azad University, Astara, Iran
[3]M.A. Student of Business Management, Rasht Branch, Islamic Azad University, Rasht, Iran
[4]Department of Business Management, Rasht Branch, Islamic Azad University, Rasht, Iran

ABSTRACT

Today Security of digital space shows a new way of each country's national security. According to role of information as a valuable goods in business, it seems necessary to protect its. For achieve this goal, each organization depending on the level of information (in terms of economic value) is required to design the information security management system until in this way could to protect their information assets. Organizations whose existence dependent on significantly on information technology can be used all tools to protect data. However, security information is required to customers' cooperation, partners of organizations and government. In this regard, it is necessary to protect the valuable information that every organization is committed to a particular strategy and implement a security system based on it. Information Security Management System is part of a comprehensive management system that is based on estimates and risk analysis, to design, implement, administer, monitor, reviewing, maintain and improve information security and its implementation have derived from Organization objectives and requirements, security requirements, procedures used and the size and structure of its organization.
KEYWORDS: Information Security Systems, Management Information Systems, Technology.

1- INTRODUCTION

Current era is called post-industrial or information era. In today's world, information is infrastructure and main factor economic and social development of countries and plays an important role in human activity. Basic technology of this era is called information technology and the latest interpretation, information and communication technology (ICT). Accelerating changes in information and communication technology so that professionals and experts in this field and also the managers decision making on ICT is require effort for maintain updating of their information. New technologies are emphasized to simplify tasks and reduce skills, but in front intelligence is focused on selection of strategies and activities planning. Acceleration of technological change is high. Alvin Toffler in future shock suggests that " If 65 to 70 years consider as a period during of a generation in past 800 years ,we understand that changes has been in more rapidly in the last generation of previous generation 799"(Alvin Toffler ، 1993). As organizations increase their adoption of database systems as the key data management technology for day-to-day operations and decision making, the security of data managed by these systems becomes crucial. Damage and misuse of data affect not only a single user or application, but may have disastrous consequences on the entire organization (Bertino & et al, 2005). Several other organizational factors that inhibit technology adoptions were also identified after conducting preliminary interviews and an extensive literature search. Among these are the cost of technology, a lack of managerial and technological skills, a lack of system integration and a lack of financial resources (Gilaninia & et al,2011;Pfeiffer, 1992; Saunders and Clark, 1992; Swatman and Swatman, 1991; Cragg and King, 1993; Iacovou, Benbasat and Dexter, 1995; Nilankantan and Scamell, 1990).

Securing Physical and Information Logic and prevent penetrate of hacker and cracker to computer networks has always been one of the problems the leading managers of organization. Outsiders sabotage on computer systems and their access to information and databases is one of the threats that need according to securing information placed as a serious priority and Information Security has raised among non-factors defense. On the other hand various provide services and e-government services, e-commerce, e-Learning and ... in area web, the information security effort will be doubled. The most important advantage of the mission computer networks is resource sharing hardware and software and a fast and easy access to information. Control access and usage of shared resources that are the most important goals of security system in a network. With the expansion of computer networks (especially Internet), attitude towards information security and other shared resources, has entered a new phase. In this regard, it is necessary any organization to protect their valuable information is

***Corresponding Author:** Shahram Gilaninia, Department of Business Management, Science and Research Branch, Islamic Azad University, Guilan, Iran. E-mail:gilani_sh45@yahoo.com

committed to a particular strategy and according to it will implement security system. The lack of a proper system of security is followed some unexpected and negative consequences. Success in securing information is depends to data protection and information systems against attack; for this reason, many security services are used. Selective service must have necessary potential about to create a protective system, timely detection of attacks, and quick response. Thus base of selected strategy can take place on the three components of protection, detection, and reaction (Hatef, 2009).

2- Information Security Management System

Information security management guidelines play a key role in managing and certifying organizational Information System (IS)(Siponen & Willison, 2009).With emergence of information security management standard occurred systematic approach to securing space of information exchange in 1995. According to this view provide security space of information exchange must be done gradual, consistent and based on a securing cycle including design, implementation, evaluation and modification.

Accordingly, each organization is required to perform secure space exchange of information as the following steps:

A- Provide organization required security plans and programs.

B- Create the organization needed to create and maintain area security of organization information exchange.

C - The implementation organization security plans and programs (Jeddi & et al, 2011).

Security standards are divided into two main categories that the first group is used in security-related terms of technical in areas such as digital signatures, public key cryptography, symmetric cryptography, hash functions, encryption functions of message authentication and, etc and the second group in relation to Security in term of management is including various parts of the organization management that management standards BS7799 is one of standards (New version of it is ISO / IEC 27001).

Table (1) - survey of standards

Standard Name	Publication year	purpose	Description
27000	2009	Basic of other standards	It consider as dictionary for other standards
27001	2005	Provide information security through explicit management	Usually used beside of ISO\IEC 27002 standards
27002	2007	Provide practical recommends for 2007 27002 information security management	Usually used beside of ISO\IEC 27001 standards and have 12 main part
27003	2010	Provide guide line and help to implementation of information security management	Including 9 main part in order to achieve his Purpose
27004	2009	Measurement, report and systematic improvement for information security	Determine how we can evaluate the performance of information security management and including 6 main part
27005	2008	Provide guide line for information security risk management	This standard support of ISO\IEC 27001 concepts. This standard don't recommend or introduce special manner risk analysis but specify structured and systematic
15408	After 1994	Provide framework to guarantee the process of recognition, implementation and evaluation of computer system done in confident and standard manner	Including 5 main part for evaluation of security

Source: www.telmarco.com/Article/ISMSScopeandAppl

Phrase information security management system is arising from regulations the ISO / IEC 27002 for information security management and is published by international organization for standardization in 2000year that will be located based on ISO 27001 standard along with other management systems standards, especially ISO 9001 and under the direct supervision and management of organization's senior management .This system is supplier of information security organization and is based on process approach. Also above system taking use implements a variety of standards and methodologies such as BS 7799 and ISO/IEC and ISO 15408(General criteria for IT) (Jeddi & et al, 2011). To establish and maintain information security management system is necessary to perform the following activities (Poole, 2007):

1. To create Information Security Management system.
2. Implementation and enforcement of information security management system.
3. Monitoring and reviewing information security management system.
4. Maintenance and improvement of management information systems.

In fact ultimate goal of ISMS system is achieve to a common point of the confidentiality, accuracy and availability.

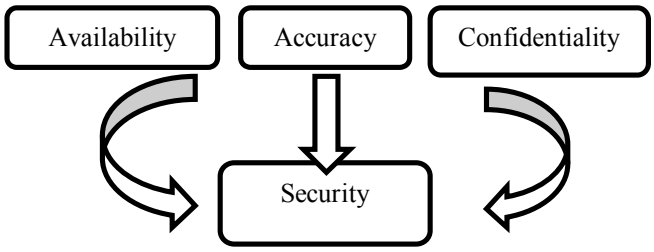

Figure 1: goal of ISMS system

3- Security Management Process

To achieve certification and to carry out the ongoing management of the ISMS it was decided to create a Security Forum. The principal duties of the security forum are measuring and continually improving compliance with the ISMS. These duties include:

- setting the ISMS scope,
- reviewing and approving all documentation associated with the ISMS,
- carrying out risk assessment and recording all changes,
- adopting security controls which reduce the security risk, consistent with the commercial imperatives of the team,
- appointing a security manager,
- conducting compliance checks against the ISMS,
- implementing and monitoring corrective actions arising from compliance checks,
- reviewing security incidents and producing a log of incident reports,
- reviewing security news

3-1-The benefits of investment in information security:

- Reduce likely to inactivation systems and programs
- Effective use of human and inhumane resources in an organization
- Reduce the cost of data loss
- Increased protection of intellectual property (Ghasemi & et al, 2007).

4- Infosec

Classification presented in this paper, information security technology is based primarily on two features:
According to a certain stage of time: This means that at the time of interaction with information technology can be proactive (active) or reaction in response necessary to a security problem.
Purpose of "proactive" is preventive action before the occurrence of a problem particular security. In such cases will be referred to the issues that will help us to prevent a problem (What should we do for ...?). Purpose of the "reactive" is necessary response after a certain problem of security (Now that ... What should we do?).
Based on implementation levels of security systems in a computer environment: information Security technology, whether from active or reactive, can be implemented at three levels:

- network level
- host level
- application level

Therefore, the security system at the network level and its services will be implemented in certain application program, or in an environment that provides the necessary conditions for the implementation of a program (host level) (Hatef, 2009).

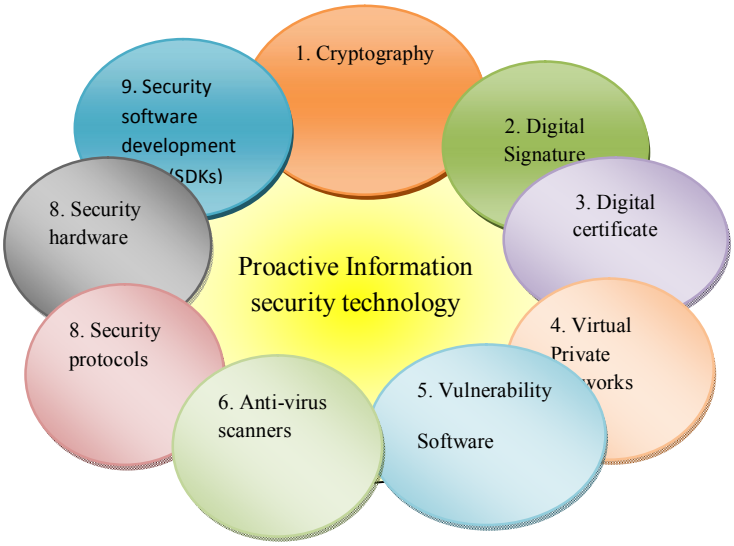

Figure 1: Proactive Information security technology (Hatef, 2009)

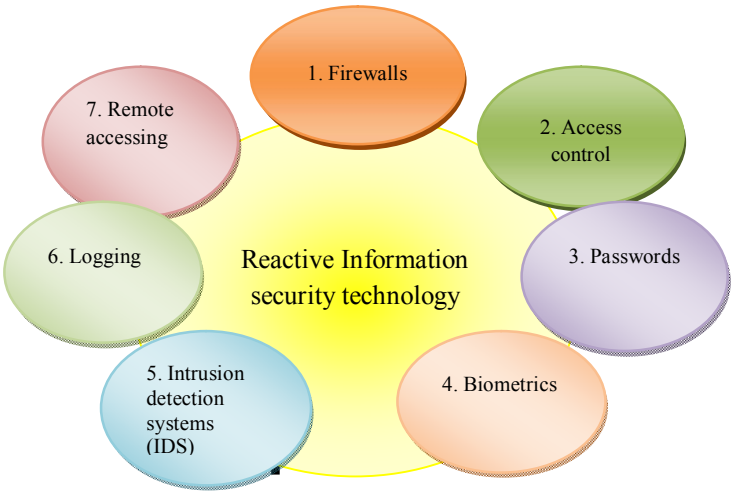

Figure 2: Reactive Information security technology (Hatef, 2009)

5- Threatening Risks of Organization Information System

Many companies try to review their managerial patterns (Gilaninia & et al, 2011).Available threats facing the security of information systems can be divided into three main categories: Confidential disclosure (disclosure), damage to the integrity of information (manipulation) and the lack of information (matching services). The most significant security threat information is disclosed. Other Threatening risks are as follows:

- Human error: the greatest amount of damage from this way is entered into the information system. Failure to provide proper training and knowledge and updated information by users and manufacturers sometimes ignored and sometimes information in their work impose heavy costs on the organization. That with proper training will be solved an important part of the issues related to data users.
- Natural disasters such as floods, earthquakes, storms and lightning.
- Systematic errors: Hardware and software problems of system that hardware problems is including inappropriate topology[1] of information network, problems related to network communications equipment (cables, routers) and stop and connect the electricity, etc and software problems are pointed to systems legacy[2]; a cavity in a software system that allows to hackers[3] attack.
- Subversive activities: Collection activities are performed by humans or machines in term of attack information systems and threatened to resources and facilities in order to destroy, alter, or disclose the information system. Illegal activities are including theft of hardware facilities and activities that are known to cybernetic crime.

[1] How to connect to computers attached together in terms of hardware
[2] Older systems that their course of benefits used is over and there isn't possible to edit them
[3] assailants that by opening encrypted information have tried to the disclosure of information, delete or change in information

- Adoption of Security policies: According to BS 7799 standard, their cases implementation of a security is as follows:
1. Determine of information security policy
2. Implement appropriate policies
3. Immediate review of current status of security information after implement security policy
4. Inspection and testing of information network security
5. Improved methods of organization information Security (Ghasemi, 2007).

6- The Need for Security Arrangements

Information system security officers must examine all information systems to determine if the system requires administration.(In the early days use of computers in shared systems was used only the username to identify individuals and there was no need to enter a password after malicious users start to abuse the system .Also passwords were added to its system. Today leadership thinks more than any other time to computers and network security. After malicious users start misuse from this system, Also passwords were added to its system. Today, leadership should think more than any other time to computers and network security. The most important reasons for this include:

• The value of investments in hardware and software equipment - computers and software packages are very expensive and replacing it is expensive and difficult. Even if in a security incident, software and hardware do not disappear completely, security problems May be forced us to reinstall all software and subsequently re-defined the basic requirements will be necessary. This is requires a lot of time especially if the person in charge don't have sufficient technical information about this area.

• The value of enterprise data - This data may include customer lists, project finance or commercial applications that are written by the user.

• The value of personal data – may be, data individual do not have little material value but losing it is very harmful and to create again information is needed a lot of time.

• The threat of computer criminals - Along with technological advances, a group of saboteurs who will benefit from the theft of computer Data have occurred. These people are causing damage and spreading distrusts and creates critical problems in the wider (Sadowsky& et al, 2003).

7- Reason Weaknesses in Security System

Software programs are often creating without considering the security issues. This issue has several reasons:

- Nonchalance- programmers and designers don't aware from the importance of security points.
- Low priority - so long ago, even those who were aware of security points compared to it didn't have much action and thus security issues were not interest really.
- Limitations of Time and cost - Some people think the security actions for the design, coding and testing have high cost in during software production process and dedicated a lot of time to their.
- Irregularities programmers - in the work of related to program the same mistakes are repeated several times and can cause security failings.
- Creative criminals - the human is creative and motivated individuals always to overcome security barriers and discovery of mistakes that led to the security failings will find a way.
- Low level of awareness - Normal users (victims of security violations) normally are not aware of the threats around them and therefore are not seek suitable ways to ensure data security and systems.
- Unrealistic view of the victims - some users are aware compared to the security points, but they are not serious them because they believed that not be performed an attack against them (Sadowsky & et al, 2003).

8- Conclusion and suggestions

Computer security is essentially a set of technological solutions for non-technical problems. Time, money and effort can be spent to secure the computer, but it can never be removed from the concerns about accidental data or intentional destruction of information. Considering the conditions set - software problem, accidents, mistakes, misfortune, bad weather or an equipped aggressive and motivated - can be seen that Each computer may take abused, the activity falls, or even completely destroyed. The task of security experts is help to organization in making decisions about time and cost that will be devoted for the issue of security. In other sectors is ensuring from appropriate policies and procedures in Organization because security budget is spent correctly. Finally, professionals should examine the system because the correct implementation of appropriate controls ensures in order to ensure to achieve objectives .thus security is more a management issue. Consequently, security should be one of the priorities of organizational management. Management should understand the security major issues and implement principles of primary security for the protection of assets.

The security plan can be divided into five distinct phase:
1. Planning for the security needs
2. Risk assessment and choosing the best practices
3. Create Policies to reflect needs
4. Implementation of security
5. Investigate and respond to events

There are two basic principles that affect in effective planning of security and policy:

In organizations, knowledge of safety and security policies should be extended from the top to down. User awareness and concerns of security issues is important; but they cannot in range organization an effective security culture create and maintain it. Instead, managers must look at security as an important issue and its rules and regulations accept and implement like other people. Effective security of computer is means of protecting from Information. In summary Information should be protected (Sadowsky & et al, 2003)

Although most organizations tend to have a secure network، provide a single definition of security that may not provide all the network requirements. Instead, each organization must evaluate the value of their data and then a security policy determine for the items that should be protected. Security system may seem expensive and time consuming but according to importance information in such a system is very essential to survival organization. In general it is necessary that organization following three conditions must be considered in the design of its information security system:

1. Ensure of information health at storage and retrieval and create opportunity for people who are authorized to use information.
2. Accuracy: information should have accuracy in term of source sent and when sending and its reread and make facilities will need to increase their accuracy.
3. Accessibility: Information for people, who are allowed to use it, should have been available and they can use information in necessity time.

REFERENCES

Alvin ,t.(1993).Future shock,translator:heshmatollah kamrani, translator Publication,

Bertino, Elisa; Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE.(2005). Database Security—Concepts, Approaches, and Challenges, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 2, NO. 1,pp2-19.

Cragg, P. and King, M. (1993). "Small-firm computing: motivators and inhibitors", MIS Quaterly, 17(1), pp.47-60.

Ghasemi shabankareh,k;mokhtari,v;amini lari,m.(2007). Security and Electronic Commerce, Fourth National Conference on e-commerce,Iran,Tehran.

Gilaninia,Sh;Chirani,E; Elham,Ramzani,Mousavian,S.J.(2011). The Impact of Supply Chain Management Practices on Competitive Advantage, Interdisciplinary Journal Of Contemporary Research In Business, VOL 3, NO 6,Pp 577-587.

Gilaninia,Sh;Danesh,S.Y;Amiri,M; Mousavian,S.J.(2011). Effective Factors on Adoption of E-Commerce in SME Cooperative, Interdisciplinary Journal Of Contemporary Research In Business, VOL 3, NO 6,pp13-21.

Hatef,M.(2009). Challenges and Prospects for Security in Cyberspace, Iranian journal of Police Human development,No 22,pp 93-117.

Iacovou, C., Benbasat, I. and Dexter, A. (1995). "Electronic data interchange and small organizations: adoption and impact of technology", MIS Quarterly, 19(4), pp.465-485.

Jeddi,M;Modiri,N;Jangjoo,M.(2011). Model for Increase Security Factor in Security Information Security Management System Based on Risk Management Using the Management Cycle Deming, Third Iranian conference on electrical and electronics engineering.

M J Kenning, 2001, Security management standard — ISO 17799/BS 7799, BT Technol J Vol 19 No 3, pp132-136.

Nilakanta, S. and Scamell, R. (1990) "The effect of information sources and communication channels on the diffusion of innovation in a data base development environment", Management Science, 36(1), pp.24-40.

Pfeiffer, H. (1992). The Diffusion of Electronic Data Interchange, Springer-Verlag, New York.

poole ,Vernon.(2007).information security management and IT audit/why the emerging ISO 27000 series are vital for business resilience.

Sadowsky ,George; James X. Dempsey; Alan Greenberg; Barbara J. Mack; Alan Schwartz.(2003). IT Security Handbook; infoDev, Worldbank; 2003. (ISBN: 964-03-9951-5; http://www.infodev-security.net/handbook)

Saunder, C. and Clark, S. (1992) "EDI Adoption and Implementation: A Focus on Interorganisational Linkages", Information Resources Management Journal, 5(1), Winter, pp.9-19.

Shabankareh,K;Mokhtari,V;Amini Lari,M.(2007). Security and electronic commerce ,the 4th e-commerce conference.

Siponen ,Mikko ; Willison ,Robert .(2009). Information security management standards: Problems and solutions,journal of Information & Management 46 ,pp267–270.

Swatman, P. and Swatman, P. (1991). "Electronic Data Interchange: Organisational Opportunity, Not Technical Problem", in Databases in the 1990's, Srinivasan, B. and Zeleznikow, J. (eds.), World Scientific Press, Singapore, pp.354-374.

www.telmarco.com/Article/ISMSScopeandAppl, modiri ,N; sobhanzadeh ,y. m, The application and scope of Information security management standards