MAT JOURNALS

Journal of Analog and Digital Devices
Volume 2 Issue 3

# A Survey: Information Security Management System

***Uranus Kazemi***
Department of Computer Engineering, Apadana Institute of Higher Education, Shiraz, Iran
Email**: uranuskazemi@yahoo.com**

***Abstract***

*It seems different organizations regarding the grade of importance of the existing information's role in them need a strong management in order to protect the security of this information. The information security refers to protecting information and minimizing unauthorized access to it. Management system of the information security means the information security of a part of general and overall information security in an organization that is based on business risks' approach and aims to establish, implement, operate, monitor, verify, maintain and improve information security. In this study, we have tried to introduce information security management system, types of threatening risks of information systems and also introduce and offer proper ways to maintain information security of each organization and then work on necessary requirements in order to design information security system and phases of implementing management system of information security.*

***Keywords:*** *Information security, organization, management.*

## INROUDUCTION

Each system needs gaining various Information and also protecting has information and secrets in order to survive and live. And the discussion of getting news and information has been common since ancient times and sometimes obtaining or disseminating information of a system have resulted in has destruction. New a days, due to raising information as a business and competitive tool as well as a profitable capital, many organization are looking for building security system to prevent information leakage to the outside in order to be able to protect their entire society in their regard, building a strong security stem can be effective for each organization's information security protection. A system that has been designed based on the organization's requirement information importance in it and it provides a protection for information assets. Information security management system (ISMS) is an appropriate tool to design and control information security [1]. In this study, we have tried to introduce information management system, kinds of threatening risks for information systems as well as offer appropriate solutions to protect each organization's Information security and after word, work on necessary requirements to design ISMS and phases of implementing ISMS.

## INFORMATION SECURITY

Information security means protecting information and information systems against unauthorized activities such as unauthorized access, use, disclosure, and reading, copying recording, destruction, revision and manipulation. Terms of information security, computer security and information are surely mistakenly applied interchangeably. Although, these topics are interrelated and all of them have common goals of protecting information confidentiality, information integration and accessibility [2], but there are subtle differences among them. Primarily, these differences are in the approach and topics which are focused an [3]. In fact, information security relates to confidentiality, integrity and availability of data, regardless of information form including electronic, print of them forms. Computer security focuses on ensuring being availability and proper functioning

of a computer system without any concern about information that is saved or processed by the computer system, government, military agencies, corporation, financial institutions, hospital and private occupations collect large amount of confidential information about employees customer, products, researches and financial condition. Most of this information is already on electronic computers collected, processed and stored and transferred in the network to other computers. If conferential information about customers and/or financial issues or new institute financial product is taken by arrival, this information leakage might lead financial loss to a business, legal pursuit and /or even bankruptcy. Protecting confidential information is a business need and in many cases a moral and legal need as well. For people, information security has a significant effect on privacy. [4]

In recent years, information security has been significantly matured and evolved. There are many ways to enter this field as a career. There are various specialized topics such as securing networks and infrastructures, securing practical applications and data bases, testing security, auditing and checking information systems, planning continuation of business and checking electronic penalties and etc. in fact information security consists securing information and minimizing unauthorized access to it and also the science of study of the methods to protect data in computer and communicative system against unauthorized change. Information security is the protecting of information for confidentiality, integrity and accessibility [5] [6]. Additionally, other features such as authenticity, responsiveness, credibility (validity), irrefutability, information reliability can also include this sort of protection.

**Security Organization Features**

A security organization encompassing three main features as the following:

- At policy- making level: leadership committee of space security of information exchanging system
- At executive- management level: space security of information exchanging system manager
- At technical level: supporting unit of space security of information exchanging system

**INFORMATION SECURITY MANAGMEN**

The Information security management is a part of Information management which its tasks are to set goals, security and consider obstacles on the way to these goals and provide necessary solutions [7].

**Information security management system (ISMS)**

An ISMS is a part of general management system in an organization that is based in business risks approach and its goal is to found, implement, exploit, supervise, maintain and improve information security. An ISMS totally is a systematic approach for managing sensitive information in order to protect it [8]. Information and security is something beyond installing a simple fire wall or tying a contract with a security-provider company. In such an approach, it is important that we balance various security activities with a common strategy in order to provide an optimal protection level.

**ISMS documentations**

Documentations which are applied in information security management include the following:

- Objectives, strategies and security policies of exchange information system space.
- Analysis plan of security risk in exchange information system space.

- Security plan in exchange information system space.
- A plan coping with security incidents and restoring them in exchange information system space
- Security awareness campaign to the system personnel
- Security training plan for personnel of the exchange information system.

**DANGERS THEARTENING INFORMATION SYSTEM**

Dangers or risks which are threatening information security can be divided into two categories: intentional and unintentional. Intentional risks attack the information security system with pre-determined plan and specific purpose such as hacker's risks. Unintentional risks are caused by human and work force errors to the system. This sort of risks puts the most damage on the information system. Risks rising from natural factors and causes such as earthquake, floods and hurricanes and etc. which including unintentional threats [9]. To eliminate existing risks in the system, firs of all. We have to think about creating information security network. To create this type of security firstly should include security policies. The items which an organization applies to implement a security system as blow:

- To determine security policy
- To apply appropriate policies
- To assess the information security condition proactively after applying security policies.
- To inspect and test information network security
- To improve methods of organization information security

**Necessary requirements for designing information security system**

Such as conditions that are needed to design information security system includes the information;

- Reliability: of information security whether during storage or retrieval and make possible for people who are authorized or allowed to use this information.
- Accuracy: information whether in terms of sending source or during its sending or reading must have accuracy and validity. And providing facilities to increase the accuracy will be needed.
- Accessibility: information for people who are allowed to use must be accessible at the times and it should be possible to use when necessary.

**Establishment stage of information security management system**

Activities related to establishing and implementing information security management system based on Deming cycle as follow:

- Establishment and designing stage
- Implementation stage
- Monitoring and reviewing stage
- Improvement and reformation stage

Activities which are operated in every phase of a project also include:

- Establishment and designing stage
- Defining initial limit(range)
- Identifying assets
- Identifying threats
- Risk assessment
- Setting a plan to handle risks
- Choosing security controls
- Setting an implementation statement

The implementation phase:

- To review for importing and finalizing the handling risk plan
- To implement the handling risk and related controls
- To review phase
- Monitoring implementation process

- Regular reviews on efficiency and effectiveness
- Monitoring acceptable risks
- Regular guidance of audits

The action phase:

- To implement improvements
- To select appropriate corrective practices
- To ensure achieving goals of improvement and develop

## THE PROCESS OF CREATING INFORMATION SECURITY MANGMENT SYSTEM

To operate information security management system, several steps are needed to be implemented [10] as following:

- To create and define policies: at this stage, creating overall policies of an organization's activities are extracted and presented in the format of document and security policy to that company key managers and expert planners will have a key role in compiling this document.
- To determine the operating scope: an organization may have several subsidiaries or branches, therefore, starting to implement information security system would be so difficult [11].to avoid the complexity of the implementation, the scope is defined which can be an organization's headquarter or an organization's official dept. or even its computer site. So, the first step will be to determine the scope and priorities for implementing a security standard in that scope and getting a certificate.
- To estimate risks: according to the list of assets and their importance for the organization, risk estimation will be done. After determining all risks for each assets, the discernment of security weak points and reasons of existing threats will be started. And afterward, weak points will be removed by getting this information and finally. Risks, threats and weak points will be documented.
- To estimate assets and their classification: to be able to apply proper controls over different department of an organization, at first, assets determination is needed. In fact, it initially must be determined what assets there are and then they should be secured. At this point, the list of all equipment's and assets of an organization is provided and the categorized according to the degree of importance [12].
- Risk managements: documents related to risks, threats and also security weak points are caused to make accurate and effective decision to cope with them [13].
- To select appropriate controls: control group has 10 control subsidiaries that which of them includes several other sub groups. By doing above steps, a company or an organization will have potential implementing controls. These ten controlling groups are as follow;
    1. Security policies
    2. The security of the organization
    3. Controlling and classification assets
    4. Individual security
    5. Physical Security
    6. Managing relationships
    7. Controlling access
    8. Methods and procedures of information maintenance and improvement
    9. Work continuity management of an organization

10. Compatibility with legal issues /cases

- To determine applicability: collecting list of assets, determining threats and security weak points and finally designing a control table help too much the procedures along. The statement of applicability (SOA) considers presenting a table called the final list of all needed controls to implement. As a result, for achieving an appropriate form of security we are inevitable to apply correct workflow which also help selecting an appropriate method and implementing a right security standard [14&15].

## CONCLUSION

It might seem difficult to apply information security system, however necessary and it has some costs which seem too much at first glance that has more benefits. Putting up this system causes to have sensitivity and better control to keep confidentiality of as system in which training and macro- planning for human forces and avoiding security information events have more effective role which is possible only through manager's support. To attract manager's support to secure information. It would be better to offer an appropriate system to get their support for strengthening information security which is a standardized and appropriate system in this regard.

## REFERENCES

1. SA, Bagheri. (2010). *Identify obstacles of implementing information security management system (ISMS) in Iranian companies Master's Thesis", Al-Zahra University, Tehran.*
2. F, Bjorck. (2001). *Security scandinavian style, interpreting the practice of managing information security in organizations*, Stockholm University & Royal Institute of Technology.
3. The White House, National Plan for Information Systems Protection Version 1.0, p.p 101 – 102, 2000.
4. A. Rathmell. (2001). *Protecting critical information infrastructures*, Computers and Security 20, p.p 43 – 52..
5. R.L. Krutz and R.D. Vines. (2001). *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, Wiley*, Washington, D.C, U.S.A.
6. P. Williams. (2001). *Information security governance*, Information Security Technical Report 6 (3), pp. 60–70.
7. B. Solms, R. Solms. (2001). *Incremental information security certification*, Computers and Security 20 (4), pp. 308 – 310.
8. R.C. Reid and S.A. Floyd. (2001). *Extending the risk analysis model to include market-insurance*, Computers and Security 20 (4), pp. 331 – 339.
9. C. Shu-The. (1990). *A study into the internationalization of national standards. Bureau of Standards*, Metrology and Inspection, Ministry of Economic Affairs.
10. J. Hoffer and D. Straub. (1989), *The 9 to 5 underground: are you policing computer crimes*, Sloan Management Review, Vol. 30 No. 4, pp. 35-43.
11. R. Filipek. (2007). *Information security becomes a business priority*, Internal Auditor, Vol. 64 No. 1, p. 18.
12. G. Dhillon and G. Torkzadeh. (2006). *Value-focused assessment of information system security in organizations*, Information Systems Journal, Vol. 16 No. 3, pp. 293-314.
13. D. Straub and R. Welke. (1998). *Coping with systems risk: security planning models for management decision making*, MIS Quarterly, Vol. 22 No. 4, pp. 441-69.
14. A. Asadi Shali. (2005). *Management of Information Security Systems*, E-

Journal of Information and Documentation Center of Iran, No. 4, Period 4.
15. H. Currangi. (2008). *Managing Information Security Systems*, Fifth Seminar on Academic Network of Western Asia, Faculty of Electrical Engineering Computer , Shahid Beheshti University.