Advances in Environmental Biology, 8(7) May 2014, Pages: 3312-3317

AENSI Journals

Advances in Environmental Biology

ISSN-1995-0756 EISSN-1998-1066

Journal home page: http://www.aensiweb.com/aeb.html

The role of human factors in information system security

[1]Leila safari and [2]Azizallah Rahmati

[1,2]Department of computer, Kangavar Branch, Islamic Azad University, Kangavar, Iran.

ARTICLE INFO

Article history:
Received 25 March 2014
Received in revised form 20 April 2014
Accepted 15 May 2014
Available online 10 June 2014

Keywords:
Information systems security, security policy, education and skills, confidence and experience of individuals, security effectiveness

ABSTRACT

Information security is a crucial issue for organizations and all organizations today are striving to maintain and improve its. The most important factors in the security of information systems and technology can be individual (human factors) cited More research which has been done in the field of view of security of information systems and technical approach and less attention has been paid to other factors involved in the security of information systems. This is in line with a new model which is called the human and organizational issues The main objective is to identify the impact of human factors in information systems security, specifically in regard to the structure of senior management support, security training, security culture, security policy, experience, confidence and skills are introduced as factors influencing the effectiveness of information systems security, The background check issue and previous studies have identified the key variables affecting the security of information systems and the proposed research are presented. Ansaty factors influencing the effectiveness of the management model for the security of information systems in organizations is provided.

To Cite This Article: Leila safari and Azizallah Rahmati., The role of human factors in information system security. ***Adv. Environ. Biol., 8(7),*** *3312-3317, 2014*

INTRODUCTION

In this study, it is felt necessary in contemporary life in organizations closely associated with their information systems. Information systems are always at risk of data theft, modification information and services are interrupting. Hence, organizations should consider information security to stay safe from damage and also information on the organizations, institutions and advanced scientific societies, is a lifeline. Information systems, simply a set of interconnected components that are data collection and processing them with the necessary information for decision making and control at various levels in the organization to provide. These components interconnected set of instructions, data, hardware and software have been formed. Classifications of information systems is proposed; Each of classified based on their goals come into the system in different groups. Classified based on the organizational structure, support systems, specific functional areas of the organization's activities are supported by systems support. Classification based on support systems, including information systems include transaction processing systems and management information systems [1]. In the book "Security Guide" states that many studies show that over 80 percent of the organization's security problems occurred due to unintentional errors and intentional staff is [2003, sadowsky et al] Transportation and control of security "employees" of the first part of BS7799 standard which emphasizes the human element in the loop of information security is the most damaging, hence considering it helps us in achieving maximum safety [2]. According to the modern national economies that are highly dependent on IT to survive today, the need for security of information and information systems is inevitable. Under these circumstances, the need to protect information and reduce the risk of much more than before and has been featured [3]. Several studies, many of the attacks have adapted to the information resources of the organization between 1998 and 2003, the number of incidents reported to the Computer Emergency Response Team of America has roughly doubled every year, 529,137 of which must be incident the report also added that only in 2003. According to Ernst & Young analysis, security events for each event can cost between 17 and 28 million dollars for the company is Since accidents are frequent and costly, management must take security seriously into consideration in order to preserve and protect information and information systems organization [4, 5, 6].

Statement of the problem:

In 1980 MIS Quarterly The results of a review of the key issues that the number of members of the Society of Information Management and a group of IT executives has been released. During the 1980s, the issue of security as a low class rank and never ranked higher than 12th in a survey in 1994 failed to earn a high was

Corresponding Author: Leila safari, Department of computer, Kangavar Branch,Islamic Azad University, Kangavar,Iran.
E-mail: Nila_safari@yahoo.com

Advances in Environmental Biology, 8(7) May 2014, Pages: 3312-3317

separated from the Security completely from the list of problem 20. However, in a study conducted in 2003, Security and Privacy high volatility found so far among the participants in this study were identified as the third issue of the degree of importance. Table 1 is a summary of how security issues are ranked in the years 1980 to 2003 show [7].

Table 1: Results of the ranking security issue [7]

Rank	Year
12	1980
18	1986
19	1989
Fall	1994
3	2003

By examining the above table it appears that security managers today as one of its main problems he sees. Security of information and information systems is a critical issue facing today's organizations around the world. The following elements of information systems security is usually defined as the basic principles of effective information security are introduced:

1 - Disclosure of Confidential Information (Disclosure)

2 - damage to the integrity Atlaghat (manipulation)

3 - The lack of information (Matching Service)

4 - human errors, which most of the damage to the information system. Failure to provide proper training and lack of awareness by users and Tvlydknndgah updated information and sometimes they do neglect impose large costs on the organization. Issues that proper training is an important part of information users will be solved.

5 - Natural disasters such as floods, earthquakes, hurricanes and lightning

6 - Objections system: hardware and software problems

7 - subversive activities: Collection activities by humans or machines to attack and threat intelligence systems and resources in order to destroy, alter or otherwise disclosing the information system is done.

8 - security policy: based on the BS7799 standard of an organization to implement a security system that acts as follows:

• define information security policy
• Appropriate policies
• Immediate check the security status of the information security policy
• Inspection and testing of network security information
• improve information organization [8]

So far, most research in the field of security of information systems ISS has been done in the field of technical and tactical been the result of attitude and see the ISS as a problem-tech research and practice research, ISS has dominated [9, 10, 11, 12, 13, 14]. Haiynd Suggests that most of the ISS research has been made, there is a vision and technical approach and Most information security professionals looking for a set of technical tools such as antivirus, firewall, etc for their security problems have been overcome. Garg Hinson Which implies that the information security technology and will take a while, there are many barriers to a mere technical approach, including:

1 - Technology is fallible;

2 - Few organizations have their own security problems well and fully understood so that they can operate based on appropriate technical solutions;

3 - The term "technical solution" encompasses a lot of money;

4 - Apart from the amount of security technologies, they can be used improperly or the users are impaired in this way lose their usefulness [14].

Few studies have been done in the field of information security models are empirically tested and Structural constraints related to behavior and human factors and organizational structures and management is handled and If the research done in this field, not due to their behavior, but behavior is the result of [15, 16].

History research:

Gonzalez human factor in information security as the Achilles' heel has been introduced [11]. IBM has stated that in 2006, while smaller attacks, concentrated and concealed information systems organizations will be more conservative. The focus of negligence and naïve users will be exploited. According to Yvyd Maki, chief knowledge Computer Rmvnk "users" as well as the weakest element of the vulnerable security models, will be abused. In 2004, two researchers, an article titled "Ten Fatal Error Information Systems Security Management" published [27] Article in the ten fault management information system were expressed as fatal errors that were ignored even one of these errors will create serious problems for a management information system Meanwhile,

the focus of these errors based on human factors and issues concerning them. Also in 2006 an article entitled "Security, Fourth Wave" fourth wave of the survey, information security has already been discussed [36].

• First wave of technology that provided the technical solutions for security issues were concerned.
• stated that the second wave of the information security management.
• The third wave of a need for formal standardization.
• A fourth wave of development firm managing information security.

All of the above should work together to ensure that the confidentiality, integrity and availability of information assets of the company, at all times has been maintained [37].

More scientists and security experts, the lack of serious research in the field of human factors has been emphasized [16] Recently, a new paradigm has emerged in the field of information security, which in the status of a "humanitarian issue" and an "organizational problem" according to [28].

Human Factors and Information Systems Security

Until the early seventies, activities related to access and protect the data stored on this information organizations and companies is limited to areas including computer LANs archives and documentsIn such environments, physical protection systems would provide information to the upper limit. In the early 80th century only a technical perspective, needed to secure and maintain computers and peripheral devices are subject to the security of knowing But over time found that most security violations through issues such as weaknesses in management and human factors is Therefore, since the mid-80s to mid-90s, was raised in the discussion that it is subject to information security management information security policy and organizational structures knew. In the mid-90s, other parameters such as defining security strategy and security policy based on the needs of the organization and its management.

In the first ten standard BS7799 Control field defines an implementation guide and it can be used as a tool to develop good structure information security. In other words, is used as the basis for hazard detection. Ten areas, including security policy, security organization established organization, asset classification and control, personnel security, physical and environmental security, continuity management, activity management, communication and operation, access control, compliance with laws and systems development and support be. And emphasize the human element in the loop of information security is the most damaging of the consideration that will help us in achieving maximum safety. Because of the high importance of human security components (factors imposed on human resources) to the component to be examined more closely. Effective indicators of human security, which can cause damage to human activities, including overwork, lack of sufficient skills, responsibilities overlap, lack of information on the value of information, lack of motivation, failure and irresponsibility forgotten something [8].

This new paradigm has emerged in the field of information security, which in the status of a "humanitarian issue" and an "organizational problem" according to [17] Different approach in line with the new paradigm of information security with a focus on providing information security behavior. Therefore, given the lack of empirical research and the importance of information security to organizations today, this study identified the factors that influence climate in search of information security in organizations that were examined in this study include the following:

• support from senior management;
• Training human factors;
• Human Factors skills;
• Experienced Human Factors;
• safety culture;
• Strengthen the policy;
• their self-esteem;
• security effectiveness.

With regard to the relationship between the individual structures on the security of information systems is quite clear and bright, primarily to be noted that the primary role of human factors information systems security is dependent on human factors.

The proposed model:

First, using a library of studies explore the issue and identify the components and parameters, and according to studies conducted on the items we have achieved a conceptual model, Which is presented as Figure 1.

Advances in Environmental Biology, 8(7) May 2014, Pages: 3312-3317

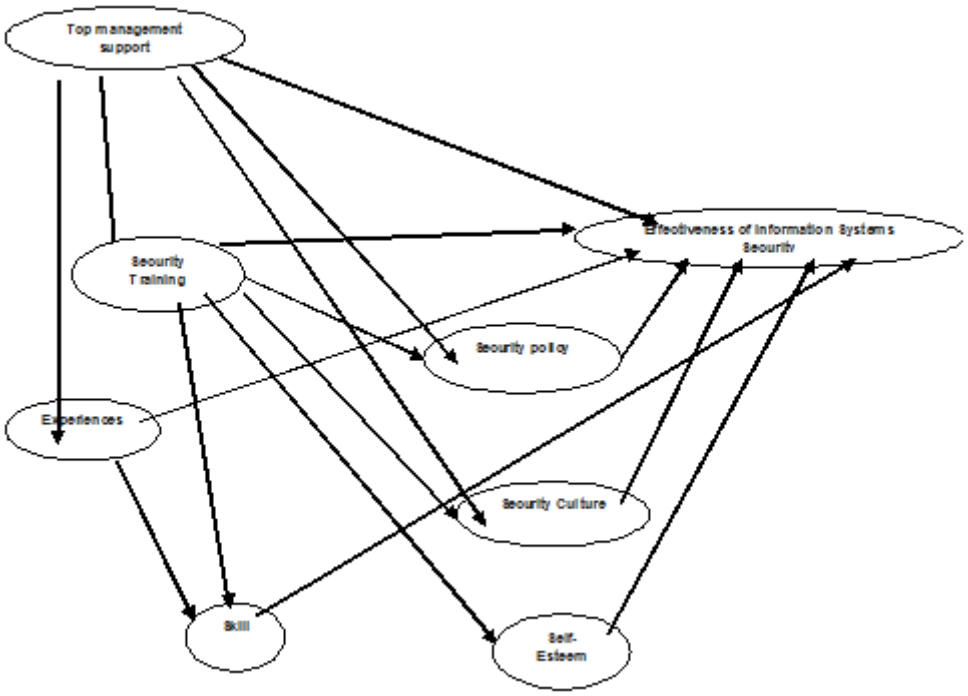

Fig. 1: models suggest

Considering that the aim of this study was to investigate the role of human factors in security for information systems model is explained and its influence on other interactive variables are considered So the proposed model is supported by senior management and the independent variables, intermediate variables, including education, skills, experience, culture, security, security policy, and is self-esteem.

In this model, the effect of simultaneously supporting senior management with respect to intermediate variables, education, skills, experience, culture, security, security policy and confidence in the effectiveness of the security of information systems will be discussed. When a positive perception of human factors training, skills, experience, culture, security, security policy, self-esteem may also excellent management of human factors with regard to the necessary support to carry out and provide leads to the effectiveness of information systems security systematic framework for the exchange of information is.

In 1998 America the federal audit reports presented to the Senate, which includes notes on the information systems security weaknesses. It was reported that "The government's reliance on information technology, the risks that may threaten national security and reduce the public service will rise" with the conviction of a federal audit, research and review many organizations U.S. government did. The results of these studies were reported: "The main weakness in information system security risk was identified risks." Finally, based on the results of this study to audit the Federal funds needed to upgrade the hardware and software equipment, staff salaries increased IT sector, the cost of training absorption propose specialists. In addition to the variables used in this study was obtained from previous studies on the effectiveness of new variables which affect the security of information systems has been identified Including the role of financial resources for the training of human resources and information systems security effectiveness is allocated mention that The excellent management of financial resources is an essential and undeniable is appropriate and timely.

Conclusions:

There is no information system that can fully establish the safety or claim it is It can be argued, however, supported by an excellent manager of factors such as: Education, skills, experience, culture, security, security policy, information systems security, self-esteem and financial resources to promote high level security and intelligence agencies maintain the highest possible standards. In addition, the study found that human factors relative to other factors (technical and tactical) has a greater impact on the effectiveness of management information systems are So we pay more attention to the factors most influence on improving the effectiveness of the security and protection of information assets in the organization have And also due to the great weaknesses of the organization in maintaining their information assets, Be compared to identify factors that affect the security of information systems and action steps to strengthen their effectiveness That is the most basic of human factors and Finally we can say that the human factor is the weakest and the weakest elements of

information systems are vulnerable to the security model that The need to strengthen the security of information systems organizations should pay special attention to human factors.

The role of human factors research on information systems security, information systems security effectiveness research conducted far beyond what they know and Need to identify the role of human factors in information system security community to be more effort.

REFERENCES

[1] Smith, H.A. and J.D. McKeen, 1992. "Computerization and management: a study of conflict and change", Information & Management, 22: 53- 64.
[2] Sadowsky, G. et al., 2003. (IT Security Handbook . infoDev. Worldbank.Wold, G.)2004(Key factors in making Information Security Policies eftfective; Available at http://cran.us.r-project.org/
[3] Schou, C.D. and K.J. Trimmer, 2004. Information Assurance and Security. Journal of Organizational and End User Computing, 16(3): i-vii.
[4] Bagchi, K. and G. Udo, 2004. An Analysis of the Growth of Computer and Internet Security Breaches. Communications of the AIS, 12(46): 684-700.
[5] Ammeter, A., C. Douglas, W. Gardner, W. Hochwarter, G. Ferris, 2002. Toward a political theory of leadership. The Leadership Quarterly, 13: 751e96.
[6] Gordon, L.A., et al., 2004. 9th Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute: San Francisco, CA.
[7] Kenneth, J., PhD. Knapp, E. Thomas, PhD. Marshall, R. Kelly, Jr. Rainer, PhD. Nelson Ford, 2005. Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness, Management Information Systems Department College of Business ,Auburn University, Alabama, USA.
[8] Specification for information security management system BS7799-2(Bishop, M.) 2003.
[9] Magklaras, G., S. Furnell, 2002. Insider threat prediction tool: evaluating the probability of IT misuse. Computers and Security, 21(1): 62-73.
[10] Kathleen, M., 2000. Carley, Information Security: The Human Perspective, Dept. of Social and Decision Sciences, Carnegie Mellon University.
[11] Gary Hinson, 2003. IsecT Ltd, Human factors in information security, Innovative information security awareness programs, Notice Bored.
[12] Jose, J., 2002. Gonzalez, Agata Sawicka, A Framework for Human Factors in Information Security, Dept. of Information and Communication Technology,Agder University College, Presented at the 2002 WSEAS Int. Conf. on Information Security, Rio de Janeiro.
[13] Marianthi Theoharidou, Spyros Kokolakis, Maria Karyda, Evangelos Kiountouzis, 2005. The insider threat to information systems and the effectiveness of ISO17799, Computers & Security, 24: 472-484.
[14] Gary Hinson, 2003. IsecT Ltd, Human factors in information security, Innovative information security awareness programs, Notice Bored.
[15] Kotulic, A.G. and J.G. Clark, 2004. Why There Aren't More Information Security Research Studies. Information & Management, 41(5): 597-607.
[16] Basie von Solmsa, Rossouw von Solms, 2005. From information security to business security?, Computers & Security, 24: 271-273.
[17] Grover, S., 2006. Kearns, The effect of top management support of SISP on strategic IS management: insights from the US electric power industry, Omega, 34: 236-253.
[18] Bhanu, S., Ragu-Nathana, Charles H. Apigianb, T.S. Ragu-Nathana, 2004. Qiang Tu, Apath analytic study of the effect of top management support for information systems performance, Omega, 32: 459-471.
[19] Danielc. Phelps, 2005. information system security: self-efficacy and security effectiveness in Florida Libraries, A Dissertation submitted to the College of Information in partial fulfillment of the requirements for the degree of Doctor of Philosophy, Spring Semester.
[20] Kankanhalli, A., et al., 2003. An Integrative Study of Information Systems Security Effectiveness. International Journal of Information Management, 23(2): 139-154.
[21] E. von Solms and Prof J.H.P Eloff, 2004. Information Security Development Trends, Department Computer Science and Information Systems, University of South Africa, Pretoria, SA.
[22] Magklaras, G.B., S.M. Furnell, 2005. A preliminary model of end user sophistication for insider threat prediction in IT systems Computers & Security, 24: 371-38..
[23] Henderson, J.C., N. Venkatraman, 1999. Strategic alignment: leveraging information technology for transforming organizations. IBM Systems Journal, 38(2,3): 472-85.
[24] Lederer, A.L., A.L. Mendelow, 1998. Convincing top management of the strategic potential of information systems. MIS Quarterly, 12(4): 525-44.
[25] Cheryl Vroom, Rossouw von Solms, 2004. Towards information security behavioral compliance, Computers & Security, 23: 191-198.

[26] Schlienger, T. and S. Teufel, 2003. Analyzing Information Security Culture: Increasing Trust by an Appropriate Information Security Culture. Unpublished, accepted on the TrustBus' workshop in conjunction with the 14th International Conference on Database and Expert Systems Applications (DEXA 2003), 2003.
[27] Basie von Solmsa, Rossouw von Solms, 2004. The 10 deadly sins of information security management, Computers & Security, 23: 371-376.
[28] Knapp, K.J., et al., 2004. Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC)2 Survey Results, Auburn University: Alabama.
[29] Gritzalis, D., 1997. A baseline security policy for distributed healthcare information systems. Computers and Security, 16(8): 709-19.
[30] Trompeter, C., J. Eloff, 2001. A framework for the implementation of socio-ethical controls in information security. Computers and Security, 20(5): 384-91.
[31] Ajzen, I., 2002. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. Journal of Applied Social Psychology, 32: 665-83.
[32] Bandura, A., 1997. Self-Efficacy: Toward a Unifying Theory of Behavioral Change. Psychological Review, 84: 191-215.
[33] Bandura, A., 1986. Social Foundations of Thought and Action: A Social Cognitive Theory. Prentice-Hall.
[34] Magklaras, G.B., S.M. Furnell, 2005. A preliminary model of end user sophistication for insider threat prediction in IT systems Computers & Security, 24: 371-38.
[35] CNN.com. 2001. The case against Robert Hanssen. In-depth special series. http://edition.cnn.com /SPECIALS/ hanssen.
[36] Basie von Solms, 2006. Information Security – The Fourth Wave, computers & security, 25: 165-168.
[37] Price Waterhouse Coopers Internet portal. 2004. Information Security Breaches Survey 2004 e technical report.!http://www.pwc .com/images/gx/eng/about/svcs/grms/ 2004 Technical_Report.pdfO.