International Journal of Science and Engineering Applications
Volume 4 Issue 6, 2015, ISSN-2319-7560 (Online)

Information System Security Model for ICT Departments

Hanieh Yaghoobi Bojmaeh
London Metropolitan University
London,United Kingdom

Abstract: Due to human theft, fraud and error is declining as well as the reduction in computer properties misuse, most of the ICT departments all, should focus on human elements in their models of information system (IS) security. This issue has not been considered in previous studies efficiently. This paper, uses qualitative approach in order to improve IS security models. Usually, in most of the developed models so far, only technical factors are considered. In this regard, an interview was conducted with 6 experts in ICT departments of 6 universities in Iran. After exact review of their ideas and insights, human factors have been identified. All of the achieved results have been added to existed technical models and then the finalized model has been designed, which was verified by experts too later. The identified human factors include staffing, training, reward and compensation system and also performance appraisal.

Keywords: Information System Security, Technical factors, Human Factors

1. INTRODUCTION

Considering so types of threats for example errors, human theft, employee error or technical failure, all are the most critical threats toward IS according to (Whiteman and Mattord, 2005). Thus, training the employees regarding information security appears to be important. Those individuals who are utilizing security monitors should be educated too and should be aware about necessity of security within a certain context since appropriate use of security monitors could be accomplished while the members are aware about security importance (Pfleeger and Pfleeger, 2003). This research, remarkably emphasizes on human and organizational factors within IS system and also computer. There would be a significant impact on information system security if both human and organizational factors influence their employment and usage with not considering the power of technical controls (Bishop, 2002).

Here, the supposed IS juncture and vulnerabilities of computer could be accomplished through a vulnerable computer and information security protection, for example, poor stability or password so as a result many harmful intentions could occur. The results of personal practices and also policies in an organization which are originated in early presumptions of design and also managerial choices would result in many susceptibilities (Besnard and Arief, 2004).

In most of the common models in IT security, the main focus is on technical elements. However, human error also should be considered. This topic has been emphasized in recent studies. However, it is important to develop a model which includes both technical and human factors. Hence, this research attempts to identify which human factors could modify the current IS security models.

2. LITERATURE REVIEW

The data availability, confidentiality and integrity are existed in IS system (Pfleeger, 2003; Bishop, 2003); the three main elements which can ensure the data security. When all of the systems constituent can be accessed only by authorized parties, so there exists confidentiality. To be aware about availability of system constituents, viewing and also printing are existed in access concept (Pfleeger, 2003; Bishop, 2003). To make sure that system's constituents can be modified by just authorized groups or manner is known as integrity. Modifications in fact are altering, forming, writing and erasing the altering position (Pfleeger and Pfleeger, 2003). Those available system constituents for the authorized people during specific times are known as availability. Moreover, denial of services will be against the availability through which accessing into defined sets of objects cannot be accepted in a certain time (Pfleeger and Pfleeger, 2003).

In general, in a framework, the first level of establishing a secured system would be identification of possible dangers. Interception, interruption, fabrication and also modification could be considered as some system dangers. These four mentioned classifications include all types of system dangers which can occur (Pfleeger, 2003). In addition, accessible information to source from the outside without any appropriate authority is known as interception. An outer source, in fact, may or may not be positioned and can be an individual, program or system (Pfleeger and Pfleeger, 2003).

Those wiretappings which are respectively successful or not successful could be the appropriate examples for both traced and non traced interceptions. When the system constituent is lost, the inaccessible and not applicable will be known as interruption (Pfleeger and Pfleeger, 2003). A good example in this regard is when the cables are connected with critical system are purposely damaged, so as a result system's connectivity would be distributed and so internal sources could not be accessible. Alteration is not only about the fact that an unauthorized person accesses a system, but instead it will modify it in such a way that is different from interception. In line with technical changes, such modifications may or may not be identified (Pfleeger and Pfleeger, 2003). The computer virus which modifies the keyboard's output is one of the good examples of what a recognizable modification is like, thus, the user will automatically becomes aware of any alterations within the system.

On the other side, users might not identify any kind of alterations in output of systems or experience if the same system is being attacked by root kit, although there are alterations of system kernel. Besides, the inclusion of counterfeit objects from an illegitimate individual is called as fabrication (Pfleeger and Pfleeger, 2003). It might not be complicated to identify due to they are the added factors, but also it is dependent on the capability of attackers too. For instance, a malevolent user, for each single transaction can

credit to his account, a very small and might be not a traceable amount by an enclosed module at server of database in a bank.

2.1. Security Threats in Information System

The threat concept is considered as all of the unexpected or potential causes of a not favorable incident that has negative impact on a system or an organization. In general, there are three main categories of threat resources:

- Natural Threats: Those events that are forces of nature such as floods, earthquakes, tornados, landslides as well as electrical storms.
- Human Threats: Those events that are both enabled or caused by humans including the intentional actions which encompass some deliberate actions and inadvertent information entry for example network based attacks, harmful software and also unauthorized access to confidential data.
- Environmental Threats: It includes those incidents or conditions such as pollution, chemical spills and also liquid leakage.

A suitable developed classification of threats would be required for explaining challenges in information security context. So far, there have been many efforts to categorize threats information system. They could be arranged according to actions or consequences. Actions might be as following types: observe, destroy, modify and emulate the threats. In addition, consequences consist of disclosure, execution, misrepresentation and repudiation of threats and also integrity threats. Moreover, the security threats can be grouped according to their involved asset types.

The other subject is about penetration techniques. Such penetration techniques could be procedural, hardware, software, physical or personal related. Other studies also defined 12 different classifications for threats such as human error acts or failure, deliberate software attacks, hardware failures and technical errors, technology obsolescence and finally natural forces.

In addition, information system threats could be assumed from two separated perspectives. The first viewpoint is according to threat agents. Such agents are authorized or classified, unauthorized groups and also environmental elements.

. 2.2. Human Errors

Because of human errors occurring by computer users, the breaches of information security might take place in many different ways. Without having any effective computer knowledge, technical errors and also careless users of computer will make many failures. Moreover, the expanding population can use computer in internet age. But also many people just describe basic facets of computer usage such as web browsing, forward email and word processing.

The significant dimensions of security measures such as firewalls, antivirus, software and patches and in addition general updates are not emphasized by most of the users (Roberts, 2004). This type of users, later easily become the main target of hackers and harmful software. Their errors might lead to compromised computers and utilized as a pad for developing major attacks of unsecured systems.

One of the important and harmful causes resulting from human failure on information security context is possibly not being careful enough. A lot of security breaches such as those users who put password on notes next to keyboards, entering into harmful websites or not assuming the demonstrated warnings by browser, as well as those workers are not able to abide security procedures and policies that could be linked to their carelessness.

In addition, more lethal dangers for firms are not emphasized and educated by the insiders. There are many dissatisfied and malevolent workers and staffs who are the victims of such attacks from social engineering. A lot of businesses could be lost because of breaches in security and many of them are linked to human errors. Moreover, many organizations may deal with more security risks initiating from not considering physical and investing on software security devices. In order to reduce human failure risks in an organization, there could be a balance among procedures, policies, technology and training (See Table 1).

Table1: Human errors by different scholars

	Limited Memory	Careless	High Workload	Policy	Password	Culture	Awareness	Employee Competition	Management Support	Security Training	Social Engineering	Education
Stanton et al., 2005					✓							
Patrick et al., 2009					✓							
Sasse, 2005					✓							
Kabanga, 2005					✓		✓			✓		✓
Neeraj, 2008					✓		✓					✓
Kraemer & Carayon, 2005								✓		✓		
Bezuidenhout, 2009	✓											
Sasse et al., 2001	✓											
Schneier 2000		✓									✓	✓
Rogers et al., 2012											✓	
Schultz 2005											✓	
Hinson 2003							✓					✓
Mees, 2006							✓					✓
Dhillon and Backhouse 2001												✓
Siponen, 2001							✓					
Sasse et al., 2006				✓		✓		✓	✓			
Adachi et al., 2007												
Kraemer , 2006			✓									
Kraemer & Carayon, 2007			✓									
Al-Fedaghi Dohery, 2008				✓								
Randa et al., 2005				✓								
Bulgurcu, 2007						✓						
Knapp , 2006									✓			

Source: Asadi (2014)

According to mentioned points above, it can be concluded that human error is a very critical factor. In following section, we will discuss on how to highlight appropriate human factors.

3. METHOD AND RESULTS

This paper applied qualitative approach to highlight the main human factors which have potential to improve information system security model. For this purpose, 6 experts were selected from ICT departments of 6 Iranian universities. They were chosen because they have enough knowledge and experience in term of information system security.

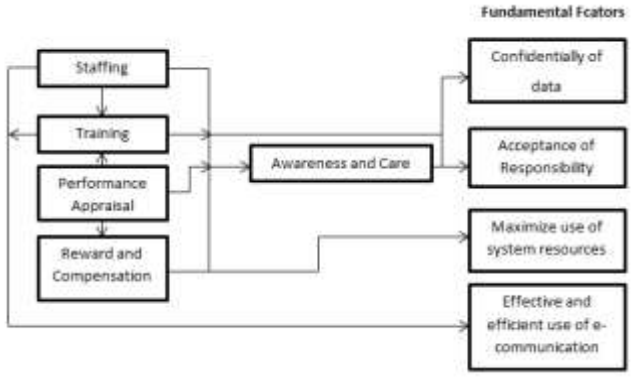
The interview process will be conducted with face to face method and open question. The questions are mainly emphasized on available technical factors and also human factors. After the interview process, all of the answers have been exactly reviewed and examined. The highlighted technical factors and human factors together with proposed model, again, have been presented to them and it was accepted by all of them. The technical factors are listed in Table 2.

Table 2: Technical factors of IS security model

Technical Factors of IS security	
Effective use of passwords	Comply for requirements
Logical access control	Responsible use of e mail and internet
Physical access control	Users (internet)
Backups	Update software
Virus prevention	System Tampering

Since size of this model is large, this paper will not demonstrate the technical factors and their relationship with each other in this developed model. Finally, the proposed model of this research will be as follows:

Figure2: Proposed model based on the human factors



Also other factors such as availability and integrity of data have been identified (as the fundamental factors). Because of the fact that these factors cannot be impacted by human factors, they are not included in this model.

4. CONCLUSION

The achieved results from this study demonstrated that in ICT departments of 6 located universities in Iran, human error can be declined through some of the human resource practices such as training, staffing, and reward system and performance appraisal. These practices, first impact information system security and care and finally will result in maximizing the fundamental factors (data confidentiality, responsibility acceptance, using the system resources and efficient and effective e-communication usage).

Moreover, integrity of data and availability of data are among those fundamental factors which are only being impacted by technical factors. In Table 2, all of the technical factors are listed. Future studies can compare the impacts of human factors and technical factors with each other. Moreover, the proposed model of current study can be adapted in healthcare industry as well.

5. REFERENCES

[1] Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & security*, *26*(4), 276-289.

[2] Besnard, D., &Arief, B. (2004).Computer security impaired by legitimate users. *Computers & Security*, *23*(3), 253-264.

[3] Bishop, M. A. (2002). The art and science of computer security.

[4] Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation.*Information Management & Computer Security*, *11*(3), 106-114.

[5] Hinson, G. (2003). Human factors in information security. *IsecT Ltd*.

[6] Kahraman, E. (2005). Evaluating IT security performance with quantifiable metrics. *Master's thesis, DSV SU/KTH*.

[7] Karyda, M., Kiountouzis, E., &Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security*, *24*(3), 246-260.

[8] Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, *14*(1), 24-36

[9] Kraemer, J. A., &Zawadowskiy, A. (2006). *U.S. Patent Application 11/499,460*.

[10] Kraemer, S., &Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, *38*(2), 143-154.

[11] Kraemer, S., &Carayon, P. (2005, September). Computer and information security culture: findings from two studies. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 49, No. 16, pp. 1483-1488).SAGE Publications.

[12] Moos, T. T. (2006). Cisco-sponsored security survey of remote workers reveals the need for more user awareness.

[13] Newman, E. (2003). Refugees, international security and human vulnerability: Introduction and Survey. *Refugees and Forced Displacement*, 3-30.

[14] Patrikakis, C. Z., Kyriazanos, D. M., Voulodimos, A. S., & Nikolakopoulos, I. G. (2009).Trust and security in Personal
[15] Network environments. *International Journal of Electronic Security and Digital Forensics*, *2*(4), 365-376.

[16] Pfleeger, C., &Pfleeger, S. L. (2003).Security in Computing 3rd.

[17] Roberts, A. S. (2004). National security and open government. *Georgetown Public Policy Review*, *9*, 69-85.

[18] Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56-62.

[19] Rupere, T., Mary, M., &Zanamwe, N. (2012).Towards Minimizing Human Factors In End-User Information Security. *International Journal of Computer Science and Network Security*, *12*(12), 159-167.

[20] Stanton, J. M., Stam, K. R., Mastrangelo, P., &Jolton, J. (2005).Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.

[21] Sarriegi, J. M., Santos, J., Torres, J. M., Imizcoz, D., &Plandolit, A. (2006). Modeling security management of information systems: analysis of a ongoing practical case. In *The 24th international conference of the system dynamics society. Nijmegen, The Netherlands*.

[22] Sasse, M. A., Brostoff, S., &Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security.*BT technology journal*, *19*(3), 122-131.

[23] Sapronov, K. (2005). The human factor and information security.

[24] Schneier, B. (2000). Software complexity and security.

[25] Schultz, E. (2005). The human factor in security. *Computers & Security*, *24*(6), 425-426.

[26] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

[27] Whitman ME, Mattord HJ., (2005) Principles of information security.2nd ed. Thomson.