INFORMATION SECURITY VULNERABILITY IN AN IRANIAN CONTEXT FROM HUMAN PERSPECTIVE
(Electrical Industry)

MALAHAT POURANSAFAR

A Dissertation Submitted In Partial Fulfillment Of The
Requirements For The Award Of The Degree Of
Master Of Science (IT Management)

Advanced Informatics School
Universiti Teknologi Malaysia

June 2013

ABSTRACT

Information security is about confidentiality, integrity and availability of the data and due to complexity of human resources the information security is always in danger of the internal threat. This study is an attempt to illustrate the importance of the human factor as an inter-organizational threat that may contribute in information security breach. The objectives of this research are to identify the human factors that may cause the information security vulnerability in Iranian electrical industry, to suggest a conceptual framework, as well as to suggest some practical solutions to deal properly with human factor and mitigate the rate of information security vulnerability in Iranian electrical industry. This research proposes a model to illustrate important human factors that may contribute in information security vulnerability. The author conducts 20 asynchronous online interviews with IT managers and their staff in IT departments of the Iranian Electrical industry. According to the findings, lack of training, lack of team working skill, having no control on emotions , having different risk perceptions, improper attitudes, improper risk communication and having demotivated staff are recognized as the significant reasons of information security vulnerability from the human angel within the Iranian electrical industry. The respondents of the study suggested some practical solutions to deal properly with human factor and mitigate the rate of information security vulnerability in Iranian electrical industry.

ABSTRAK

Keselamatan maklumat adalah mengenai kerahsiaan, integriti dan ketersediaan data dan kerana kerumitan sumber manusia keselamatan maklumat sentiasa dalam bahaya ancaman dalaman. Kajian ini merupakan satu cubaan untuk menggambarkan betapa pentingnya faktor kemanusiaan sebagai ancaman kepada inter-organisasi yang boleh menyumbang kepada pelanggaran kepada sistem keselamatan maklumat. Objektif kajian ini adalah untuk mengenal pasti faktor-faktor kemanusiaan yang boleh menyebabkan kelemahan kepada sistem keselamatan IT dalam industri elektrik Iran. Juga, untuk mencadangkan satu rangka kerja konsep dan membangunkan ia dalam pendekatan deduktif. Serta, untuk mencadangkan beberapa penyelesaian yang praktikal dalam menguruskan faktor kemanusiaan dengan betul dan mengurangkan kadar kelemahan kepada sistem keselamatan maklumat di dalam industri elektrik Iran. Kajian ini mencadangkan satu model untuk menggambarkan faktor-faktor penting kemanusiaan yang boleh melemahkan sistem keselamatan maklumat. Penulis telah menjalankan 20 temu bual dalam talian segerak dengan pengurus-pengurus IT dan kakitangan di bahagian IT di jabatan industri elektrik Iran. Hasil temu bual menunjukkan bahawa kekurangan latihan, kekurangan kemahiran kerja berpasukan, tidak mempunyai kawalan ke atas emosi, mempunyai persepsi risiko yang berbeza, sikap yang tidak betul, risiko komunikasi yang tidak wajar dan mempunyai kakitangan yang tiada motivasi adalah punca kepada kelemahan sistem keselamatan maklumat dari sudut kemanusiaan dalam industri elektrik Iran. Responden-responden dari kajian ini telah mencadangkan beberapa penyelesaian yang praktikal untuk berurusan secara betul dengan faktor kemanusiaan dan mengurangkan kadar kelemahan keselamatan maklumat dalam industri elektrik Iran.

TABLE OF CONTENTS

LISTS OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

IT	-	Information Technology
IEIS	-	Iranian Electrical Industry Syndicate
OCTAVE	-	Operationally Critical Threat, Asses and Vulnerability Evaluation

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, application of IT as a strong enabler that leverages enterprises and create sustainable advantage is increased across the globe. In several organizations, the information became an important source of analyzing the market situation, rivalry among competitors and several important data to gain competitive advantage. Several organizations are highly depended to the information system to conduct their business in a professional manner (Peppard & Ward, 2004).

In order to keep the information confidential, correct and accessible in different access levels, the information security is practiced by the experts to mitigate the information security challenges within the organizations. Although several solutions were initiated to reduce the human, organizational and technical challenges of information security, but still many organizations are struggling with information security breaches. On the other hand, implementing information security is a costly process and cannot assure full protection of the information from unauthorized access (Van der Leeden, 2010).

1.2 Background of the Problem

There are several challenges and obstacles for implementing an information security system in organizations. The challenges are not only related to the technological factors, but also the influences of organizational and human elements are very considerable (Werlinger, Hawkey, & Beznosov, 2009).

In order to conduct a root cause analysis about the security vulnerability , it is important to have a deep insight into the human, organizational and technological factors and their interactions that make cause security breaches, whether directly or indirectly (Kraemer & Carayon, 2007).

Implementing technology is important to protect the enterprise information transaction but it is impossible to secure it without organizational and human supports. In other word, the attitude of the staff is always a critical to support the information security, but the inter-organizational processes and managerial commitments are also significant to align the human efforts with the objectives of the information security systems (Dutta & Roy, 2008).

According to Ifinedo (2012), several organizations have been failed to implement a secure information system because they have a very shallow insight into the potential threat of the staff. In several cases, it is found that several workforces prefer to avoid security stages and processes for faster access to the organizational data. In fact the human resources are internal threats of the companies and it is vital for the organizations to concentrate this significant factor to avoid Information Security breaches and all associated factors.

Among the security breaches that caused by human factor, just a few of them are generated intentionally or purposely. In fact, usually the users of the information systems are not aware of consequences of security vulnerability and due to the lack of knowledge they usually do not care about the formal security procedures and create unintentional errors (Alder, Noel, & Ambrose, 2006).

Many researchers have highlighted that half of the human who maid failures in security systems are not created purposely. Indeed, the lack of knowledge or unawareness is the typical reason for sabotage in security systems (Vroom & von Solms, 2004).

An academic case study that has been conducted by (Kazemi, Khajouei, & Nasrabadi, 2012) about the information security success factors in Iranian Public sectors, argues that the issue of information security is very sensitive in municipal organizations because the private information about individuals are recorded in databases and the threats of information lost, unauthorized access to databases and the security vulnerability is serious. In such organizations the staff needs to be well informed about the consequences of the security breach through intensive training programs. Nevertheless, demotivated and irresponsible work forces are considered as inner potential threats that may contribute in information security sabotage. Furthermore, the initiation of the supportive programs to protect the information security systems via training and awareness sessions, award and penalty approaches, employee engagement and empowerment, etc., is impossible without the ultimate support of the top management and the maturity alignment between corporate and IT governances.

1.3 Problem Statement

Implementing information security system in organizations is the most challenging task of IT managers. It is obvious that proper implementation of the information security system can classify the organizational data and provide a proper access level for each of the staff based on their position and role in the organizational hierarchy. The role of the information security system is not only related to the internal data exchange but the safety of the external data exchange is another issue that the IT managers should be cautious about that. The author has found several problems and challenges of Information security systems that are related to the human element and the employee may contribute to the security breaches due to the several reasons including unawareness and lack of proper training, demotivation, improper risk communication, conflict in risk perceptions, negative personal attitude, cultural barriers and lack of relevant experience.

According to the importance of the human role in implementing information security systems, as well as due to the insufficient studies about the human factors that may cause information security challenges in Iranian electrical industry, the author has attempted through this dissertation to identify the main human factors in an Iranian context for the purpose of suggesting a conceptual framework to facilitate further studies.

1.4 Purpose of the Study

A review of the conducted studies reveals that there are many security challenges related to the Human, Organizational and Technological factors as well as their interaction during implementation of information security systems in the organization (Werlinger, Hawkey, & Beznosov, 2009). According the study has been conducted by Botta , et al. (2007), the human factor has a significant role in the design and implementation of the security systems. On the other hand the role of management is important to implement the information security system with a maximum contribution of the human resources. The risk management process and use of cultural theory is important to classify the different aspects of security risks related to human factor (Vaughn Jr, Henning, & Fox, 2001). There is a lack of enough information about the impacts of organizational factors such as the size of the company, top management support, and type of industry. So a holistic framework is necessary to reveal the influences of those factors on the effectiveness of information security controls within organizations (Kankanhalli, Hock-Hai, Bernard, & Kwok-Kee, 2003).

The purpose of this study is to illustrate the human factor that may contribute in information security vulnerability.

1.5 Objective of the Study

The objectives of this study are as follows:

- To identify the human factors that may contribute on information security vulnerability in Iranian electrical industry.
- To propose a framework about the impact of human factors on information security vulnerability in Iranian electrical industry.
- To analyze the impact degree of human factors on information security systems in the context of the Iranian electrical industry.
- To suggest some practical solutions in order to mitigate possibility of the information security vulnerability made by human factors in Iranian electrical industry.

For this purpose, the author adopts the human factors from a holistic framework of Werlinger, et al. (2009) . Also, the author conducts several interviews with the information security experts in order to add more factors. Eventually the respondents of the study evaluate the suggested model by weighing the impact degree of each item and proposing additional human factors that may influence the information security systems in Iranian Electrical industry.

1.6 Research Questions

The author proposed some preliminary human factors by adopting the holistic framework of Werlinger, et al., and brainstorming with several practitioners. The followings are the research questions to comply with this study:

1. What human factors usually contribute in information security vulnerability in Iranian electrical industry?

2. What is the proposed conceptual framework of information security vulnerability in Iranian electrical industry?

3. What aspect of human factors is most concern to information security vulnerability in Iranian electrical industry? (Weighing each factor)

4. What are the practical solutions to mitigate possibility of information security vulnerability made by human factors in Iranian electrical industry?

1.7 Scope of the Study

This study focuses on the human challenges that may cause information security vulnerability in Iranian organizations (electrical industry). This study analyzed the challenging human factors for implementing information security systems in Iranian electrical companies that are officially registered under the Iranian Electrical Industry Syndicate (IEIS) (appendix c), based on the suggested framework of the author.

However, since the framework was emergent, this study was an attempt to identify the other human challenges in the Iranian context to develop that framework.

In this study the author applied purposeful and convenience sampling to collect the qualitative data via asynchronous online interview among the staff of IT department of some companies that are registered in IEIS to cover the primary data of the research.

1.8 Significance of the Study

According to the IT practitioners in IEIS companies, there is no specific study about the impact of human factors in information security systems of IEIS members, the results of this study are important for Iranian information security practitioners as well as for top management of the Iranian companies, especially the IEIS members. So, this research can provide a deep insight into the existed human challenges for implementing information security systems. Moreover, the suggested conceptual framework could be useful for future studies.

1.9 Summary

The author found through previous studies that the human factor is an inter-organization threat that may contribute in security breaches, whether intentionally or unintentionally. The study suggested a conceptual framework of the human drivers that cause many security vulnerabilities in Iranian Electrical organizations. The outcome of this research and the suggested framework could facilitate further researches in other industries across the globe. Furthermore, the IT practitioners as well as the top management of the Iranian Electrical industry may refer to the findings of this thesis to have proper insight into the importance of the human factor to mitigate the challenges of the information security breaches.

References

Al-Awadi, M., & Renaud, K. (2007). SUCCESS FACTORS IN INFORMATION SECURITY IMPLEMENTATION IN ORGANIZATIONS. *IADIS International Conference e-Society.*

Alberts, C., & Dorofee, A. (2003). *Managing Information Security Risks The OCTAVE Approach.* Boston, USA: Pearson Education, Inc.

Alder, G. S., Noel, T. W., & Ambrose, M. L. (2006). Clarifying the effects of Internet monitoring on job attitudes:The mediating role of employee trust. *Information & Management*(43), 894–903.

Ashenden, D. (2008). Information security management: a human Challenges? *Elsevier Information Security Technical Report*(13), 195 - 201.

Benson, C. (2013). *Security Threats*. Retrieved Feb 12, 2013, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc723507.aspx

Blythe, J., Camp, J., & Garg, V. (2011, 02 13). *Targeted Risk Communication for Computer Security.* Retrieved Dec 20, 2012, from University of Southern California: http://www.isi.edu/~blythe/papers/pdf/blythe-risk-communication.pdf

Bosworth, S., Kabay, M. E., & Whyne, E. (2009). *Computer Security Handbook* (5th ed.). New Jersey: Wiley and Sons, Inc.

Botta, D., Welinger, R., Gagne, A., Beznosov, K., Iverson, L., Fels, S., et al. (2007). Towards Understanding IT Security Professionals and Their Tools. *Symposium On Usable Privacy and Security*, 100-111.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data System*, *106*(3), 345-361.

Dutta, A., & Roy, R. (2008). Dynamics of organizational Information security, System Dynamics Review. *WILEY*, *24*(3), 349-375.

Egan, M. (2005). Information Security and Human Factor. *Online Journal of Information Systems Audit and Control Association, 3*.

Eminagaoglu, M., Ucar, E., & Eren, S. (2009). The positive outcomes of information security awareness training in companies - A case study. *Information Security Technical Report*(4), 223 - 229.

Goleman, D. (2012, June 22). *Social Intelligence*. Retrieved Jan 13, 2013, from Goleman's model of emotional intelligence: http://danielgoleman.info/golemans-model-of-emotional-intelligence/

Government of the Hong Kong . (2002). *What is Information Security*. Retrieved Nov 11, 2012, from INFO SEC: http://www.infosec.gov.hk/english/information/what.html

Hassell, L., & Wiedenbeck, S. (2004). *human factor and information security.* College of Information Science and Technology. Philadelphia: Drexel University.

Hayden, L. (2010). *Human Information Security Behaviors: Differences Across Geographies and Cultures in a Global User Across Geographies and Cultures in a Global UserSurvey* (Vol. 46). American Society for Information Science and Technology.

Hinson, G. (2003). *Human Factor in Information Security.* IsecT Ltd., Innovative Information Security Awareness Programs, Holmbury St.Mary.

Hinson, G. (2003). *Human factors in information security.* Retrieved 10 7, 2012, from http://www.noticebored.com

Hoepfl, M. C. (1997). Choosing Qualitative Research: A Primer for Technology Education Researchers. *journal of Technology Education, 9*(1).

Hofstede, G. (1984). Cultural Dimentions in Management and Planning. *Asian Pacific Journal of Management, 1*(2), 81-89.

Ifinedo, P. (2012, February). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 13*(1), 83-95.

IT Governance Institute. (2007). *COBIT 4.1.* Retrieved April 05, 2013, from Information Systems Audit and Control Association, ISACA: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

Johnson, S. D. (1995). Will our research hold up under scrutiny? *Journal of Industrial Teacher Education, 32*(3), 3 - 6.

Kankanhalli, A., Hock-Hai, T., Bernard, T., & Kwok-Kee, W. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management*.

Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. *African Journal of Business Management*, *6*(14), 4982-4989.

Kets de Vries, M. (2001). The anarchist within clinical reflections on Russian character amd leadership style. *Human Relations, 54*(5), 585-627.

Khosravi, B. G., Manafi, M., Hojabri, R., Farhadi, F., & Gheshmi, R. (2011). The Impact of Emotional Intelligence towards the Effectiveness of Delegation: A Study in Banking Industry in Malaysia. *International Journal of Business and Social Science, 2*(18), 93 - 99.

Kissel, R. (Ed.). (2011). *Glossary of Key Information Security Terms.* Diane Publishing.

Koskosas, I. V., & Paul, R. J. (2004). The Interrelationship and Effect of Culture and Risk Communication in Setting Internet Banking Security Goals. *6th international conference on Electronic commerce* (pp. 341-350). New York: ACM.

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.

Kruger, H. A., Flowerday, S., Drevin, L., & Steyn, T. (2011). An Assesment of the Role of Cultural Factors in Information Security Awareness. (pp. 1-7). Potchefstroom: Information Security South Africa (ISSA).

Lacey, D. (2009). *Managing the human factor in information security:how to win over staff and influence business managers.* chichester: Jhon Whiley and Sons, Ltd.

Maçada, A. C., & Luciano, E. M. (2010). The influence of human factors on vulnerability to information security breaches. *Americas Conference on Information Systems* (pp. 1-9). Lima: AMCIS .

McShane, S. L., & Von Glinow, M. A. (2012). *Organizational Behavior, Emerging Knowledge and Practice for the Real World* (5th Edition ed.). Boston: McGraw-Hill.

Mitnic, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security.* Indiana: Wiley Publishing, Inc.

Niekerk, J. V., & Solms, R. V. (2005). AN HOLISTIC FRAMEWORK FOR THE FOSTERING OF AN INFORMATION SECURITY SUB-CULTURE IN ORGANIZATIONS. *Information Security South Africa (ISSA).*

O' Reilly, C. A., & Chatman, J. A. (1996). Culture as a Social Control: Corporations, Culture and Commitment. (B. M. Staw, & L. L. Cummings, Eds.) *Research in Organizational Behaviour, 18*, 175 - 200.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *40th Annual Hawaii International Conference on System Sciences (HICSS'07).* IEEE.

Parker, D. (1998). Organizing for Security. In D. Parker (Ed.), *Fighting Computer Crime, A New Framework for Protecting Information.* John Wiley & Sons.

Parsons, K., McCormac, A., & Butavicius, M. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment.* Edinburgh South Australia: Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation.

Peppard, J., & Ward, J. (2004). Beyond strategic information systems: towards an IS capability. *Journal of Strategic Information Systems, 13*, 167–194.

Pouransafar, M., Cheperli, M., & Faraj Tabrizi, M. R. (2013, Apr). Failure Factors of ERP Projects in an Iranian Context. *IOSR Journal of Business and Management, 9*(4), 83 - 87.

Sasse, M. A., Brostoff , S., & Weirich, D. (2001). Sasse MA, Brostoff S, Weirich D. Transforming the 'weakest link' a human/computer interaction approach to usable and effective security. *BT Technology, 19*(No. 3), 122 - 131.

Snedaker, S. (2006). *Syngress IT Security Project Management Handbook.* (R. Rogers, Ed.) Rockland: Syngress Publishing, Inc.

Tarimo, C. N. (2006). *Information Security in Under Developed Countries: A Social-Technical Approach.* Stockholm: Department of Computer and System Sciences-DSV ,Stockholm University/ Royal Institute of Technology.

Tohidi, H. (2011). Human resources management main role in information technology project management. *Procedia Computer Science, 3*, 925 - 929.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2006). Formulating information systems risk management strategies through cultural theory. *Information Management & Computer Security, 14*(3), 198 - 217.

Vacca, J. R. (2009). *Computer and information security handbook.* (J. R. Vacca, Ed.) Boston: Elsevier.

Van der Leeden, K. (2010). *Security without risk?Investigating information security among Dutch universities.* University of Twente, School of Management and Governance. Enschede: Unpublished MasterThesis.

Vaughn Jr, R. B., Henning, R., & Fox, K. (2001). An empirical study of industrial securityengineering. *The Journal of Systems and Software, 61*(3), 225-232.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural. *Computer & Security*(23), 191-198.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). Human, Organizational, and Technological Challenges of Implementing IT Security in Organizations. *Information Management& Computer Security, 17*(1), 4-19.

WordPress. (2012, Murch). *Fishbone Diagram*. Retrieved April 3, 2013, from VectorStudy: http://vectorstudy.com/management-theories/fishbone-diagram

Zafar, H. (2013). Human resource information systems: Information security concerns for organizations. *Human Resource Management Review, 23*, 105 - 113.