VALUE FOCUSED ASSESSMENT OF INFORMATION SYSTEM SECURITY

SAMAN ASADI

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JANUARY 2014

I dedicated this thesis to my beloved Mother, Father, and Brother for their endless supports and encouragements.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my utmost gratitude to my supervisor, **Dr. Norafida Ithnin** being a dedicated mentor as well as for her valuable and constructive suggestion that enabled this project to run smoothly.

Last but not least, I am forever indebted to all my family members and my best Friends, Ali FT, Ba Bak, Ghasem, Aida, Amirhossein, Shervin, Bright, Saeed Sol, Aboozar and Negar for their constant support throughout the entire duration of this project. Their words of encouragement never failed to keep me going even through the hardest time and it is here that I express my sincerest gratitude to them.

ABSTRACT

Because of decline in human theft, error, fraud and also misusing the computer properties, the approach of value focused thinking needs to be established. A powerful IS or information system is not able to be developed just according to its technical abilities. This project concentrates on bringing a lot of reliable security system of IS and recognizing the core parts by means of value focused thinking method. Mean and fundamental goals are the outcomes of this method in which the core objectives all have some general usage for decision making in planning of security. The basic objectives have a tight relation with acknowledged aims of the information system security for instance confidentiality and integrity and the mean goals are generally about social challenges for example being responsible for using the sources effectively. In this project, value focused was used in order to develop the current model of the scope. In this regard 6 individual experts were asked to participate and by asking them some questions, fundamental objectives of the organization extracted. Then a new model was presented and this model before being distributed among the staff as a questionnaire was shown to 6 experts and they confirmed it. After their confirmation, this new model was tested by means of questionnaire and the results were analyzed by using the SPSS software.

ABSTRAK

Oleh kerana pengurangan dalam kecurian manusia, kesilapan, penipuan dan juga penyalahgunaan sifat-sifat komputer, pendekatan kepada nilai berfokuskan pemikiran perlu diwujudkan.Sistem maklumat yang kuat tidak dapat dibangunkan hanya mengikut kebolehan teknikal. Projek ini menumpukan kepada membangunkan lebih banyak sistem keselamatan maklumat yang boleh dipercayai dan mengiktiraf bahagian teras melalui kaedah pendekatan kepada nilai berfokuskan pemikiran . Maksud dan matlamat asas adalah hasil kaedah ini di mana semua objektif teras mempunyai beberapa penggunaan umum untuk membuat keputusan dalam perancangan keselamatan. Objektif asas mempunyai hubungan yang rapat dengan mengakui keselamatan sistem maklumat seperti kerahsiaan dan integriti dan maksud matlamat adalah secara umumnya mengenai cabaran sosial contohnya bertanggungjawab dalam menggunakan sumber-sumber dengan berkesan. Di dalam projek ini, pendekatan kepada nilai berfokuskan pemikiran telah digunakan untuk membangunkan skop model semasa. Untuk itu, 6 orang pakar telah diminta untuk mengambil bahagian dan dengan memberi beberapa soalan, kami mencapai objektif asas organisasi. Kemudian model baru telah dibentangkan dan model ini sebelum diedarkan di kalangan kakitangan sebagai soal selidik ianya telah disahkan oleh 6 orang pakar tersebut. Selepas pengesahan mereka, model baru ini telah diuji melalui soal selidik dan keputusan telah dianalisis dengan menggunakan perisian SPSS.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Assuming some of the threats for instance human theft, errors, employee error and technical fail are the most important threats to IS (Whitman and Mattord, 2005). Therefore educating the members about the information security seems crucial. The individuals who are employing security monitors need to be trained and also to be aware about security's importance in a specific context due to having sufficient usage of security monitors can be done while the staff know about necessity of security (Pfleeger and Pfleeger, 2003). This study mainly focuses on organizational and human elements inside the information security system and computer. There will be a drastic impact on security if both organizational and human elements affect their usage and employment with not respecting the technical controls power (Bishop, 2002). In this regard, the considered juncture of IS and computer vulnerabilities might be done by a vulnerable computer and also IS protection for instance weak usability or poor password so some harmful intentions might happen. The outcomes of individual practices and organizational policies that their origins are inside the early design presumptions as well as management choices will lead to susceptibilities (Besnard and Arief, 2004).

1.2 Background of the Study

B Nowadays, all organizations are trying to increase their performance by using IT (Popova and Sharpanskykh, 2010; Smart and Conant, 2011; Walker et al., 2011). Some researches tried to identify the important factors and impact of these factors on IT acceptance, for example, Venkatesh and Davis (2000); Holden and Karsh (2010) by using managerial view identified important factors on employee performance and impact of these factors on IS security. Also some researches have been done for evaluating the impact of IT on knowledge sharing, most of these researches used knowledge sharing for achieving higher innovation (Maier and Hädrich, 2011; Choi et al., 2010).

However, the importance of IT and its advantage causes to researches study on it from different views. Surely so many researches study IT from engineering side and information system security is a most important of these researches. Information in all organizations is important and ISS trying to protect this important (Ling and Masao, 2011).

The outcomes of managed IS security, concentration on information system security study moves higher than the technical perspective and it can be close to organizational and individual point of view for having general objectives inside the system. Regarding organizational level there is no growth for the information security breaches in IS and happening of the risks that can threat individuals inside the firm. Also for having sufficient understanding of information system security in area of ethics, is according to mentioning it at the level of combination of the organization and technology. According to Segev et al. (1998) statement, the key of the security is not about technology, but rather the organization. Also it should be noted that IS security at organizational and technical level (Trom peter & Eloff, 2001) as well as its establishment needs to have cognizance of both human and ethical assumptions.

In general, the important values of individuals that are core of objectives which will be developed, the clarified organizational and social definitions and their elements have their main roles as well. As mentioned by Keeney (Keeney, 1992), providing values for the consciousness lets you to clarify the hidden goals, the ones you did not know you had before.

The IS security cornerstone goals which are the foundation of activities of secure system in past and the crucial reason for developing methodologies that integrity, confidentiality and also the data availability needs to be followed by the value measures for avoiding inability issues related to managing IS security. So in this case, the method of combining different organizational and social elements to make sure security of IS was assumed.

1.3 Statement of the Problem

The IS or information system security will continue to show some extent of challenge related to professionals and executives. A bigger part of the information system security study is naturally technical with a little assumption of organizational and individual challenges. These days unfortunately, a lot of firms do not have sufficient attention to the individual value and they only concentrate on technical parts. Because of technical failures and human errors, organizations need to be aware about crucial role of education of staff for enhancing the information system security.

Because a lot of firms apply and use advanced technology for their security system for instance biometrics and smart cards, the external threats will not be assumed as the key issues of the IS (Kreicberge, 2010 and Leach, 2003). According to Leach (2003), the important challenges are about some of the internal threats like errors of users, their carelessness and also omissions that are all resulted by internal elements as the behaviors of week users. Based on some researches, in a lot of

security breaches staff inside a firm could be assumed unintentionally or intentionally (Kreicberge, 2010, Siponen et al., 2010). The guilty role of the staff is a point that is assumed as an internal threat. Based on Boujettif and Wang (2010), four out of five security incidents in firm are the result of internal threats. Some of them in Malaysia will proof this fact as well. For instance, human error is a crucial internal threat in using Health Information System of the Malaysia (Samy, 2010, Humaidi, &Balakrishnan, 2013).

According to some studies, in so many security breaches employees in an organization can be guilty intentionally or unintentionally (Kreicberge, 2010, Siponen et al., 2010). Employees' guilty role is something that is an internal threat. As Boujettif and Wang (2010) reported 4 out of 5 security incidents in organizations are caused by internal threats. Some researches in Malaysia support this fact. For example, human error is one of main internal threats in applying Health Information System in Malaysia (Samy, 2010, Humaidi, & Balakrishnan, 2013).

For as much as technical and human factors and relation between these factors in order to improve ISS in healthcare industry in Malaysia is not clear, this study attempts to show how technical and human issues can improve the information system security in these industries.

1.4 Purposes of the Study

According to the past studies which was accomplished in IS area, a lot of concentration is for the technical aspect in nature and there exist a little focus of value measures and the organizational challenges. Also the managed IS security shows a sufficient challenge for the executives and organizations. Here, technical borderline was passed and value of individuals for using a wider organizational view is assumed. It means that the aim of this project is employing value focused thinking

for core objectives of the information system security and will add more new elements for enhancing the IS security.

1.5 Objectives of the Study

Because of the enhanced concern for the study of IS security inside the firms and slowly growing the breaches of IS security, the join of organization and technology levels both need to be assumed to approaching the IS security which is managed. Obviously, having some realization into a wider view could be done if the managers have more focus on individual issues rather than technology. For approaching past objectives of the current project, the study in previous investigations that were relevant to this field was developed and also their approaches were compared to each other and the improvements of the hospitals was done. For conclusion, the goals could be defined as below:

(i) To define general goals in IS security through value focused thinking.
(ii) To improve the current model for obtaining more value for keeping IS security.
(iii) To measure the effects of elements impacting IS security.

1.6 Research Questions

Research question 1: What are the general goals in ISS of health care industry of Malaysia?

Research question 2: How value focused is able to improve current model for getting more value for keeping information system security?

Research question 3: What is the impact of highlighted elements impacting IS security?

The main significance of this study is the fact that each work which was accomplished until currently is not able to be totally secured in opposite of each kind of available threats and a lot of them are concentrating on technical security and also ignore organizational perspective and people value. In addition, the previous techniques and also methods were not able to cover this idea which was the important disadvantage from them which is implemented and studied. Although there are some suggested approaches like value focused, was not used for hospitals. For conclusion, value focused thinking evaluation inside the hospitals and making them more secured is assumed as the main importance of this study.

1.7 Scope of the Study

The scope for current research is the Malaysia health care industry. For achieving this goal the hospitals of Malaysia are the target of the research. They are all located in Kuala Lumpur. Four hospitals will be studied in this project, two privet hospitals and two government hospitals. Because of following reasons these hospitals will be set as a scope: first, healthcare industry should in accordance with approved rules by government, so the base of IS security is same in all hospitals. Second, value focused thinking is a method that it can extract current model and situations, and according to experts experience and ideas, it will improve current model. So value focused can improve ISS in hospitals. Third, improving current model will help this project to achieve the stronger model than current model by

evaluating private and government hospitals, because it will use both of systems and their experts' experience.

REFERENCES

Armstrong, H., 1999 A soft approach to management of information security. Unpublished PhD thesis, School of Public Health, Curtin University, Perth, Australia.

Backhouse, J. &Dhillon, G., 1996 Structures of responsibility and security of information systems. European Journal of Information Systems, 5, 2–9.

Barrett, M. &Walsham, G., 1999 Electronic trading and work transformation in the London Insurance Market. Information Systems Research, 10, 1–22.

Baskerville, R.L., 1991 Risk analysis: an interpretive feasibility tool in justifying information systems security. European Journal of Information Systems, 1, 121–130.

Baskerville, R.L., 1989 Logical controls specification: an approach to information systems security. In: Systems Development for Human Progress, Klein, H.K. & Kumar, K. (eds), pp. 241–255. Elsevier Science Publishers, Amsterdam, the Netherlands.

Boujettif M, Wang Y 2010 Constructivist Approach to Information Security Awareness in the Middle East. Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference.

Boxx, W. Randy., Randall Y. Odom., and Mark G. Dunn. 1991. "Organizational values and value congruence and their impact on satisfaction, commitment, and cohesion: an empirical examination within the public sector." Public Personnel Management 20 (1), 195-205.

Calori, R., Johnson, G. &Sarnin, P., 1992 French and British top managers' understanding of the structure and the dynamics of their industries: a cognitive analysis and comparison. British Journal of Management, 3, 61–92.

Chatman, J.A., 1991 Matching people and organizations: Selection and socialization in public accounting firms. Administrative Science Quarterly, 36, 459-484.

Chatman, Jennifer A., 1989 Improving interactional organizational research: A model of person organization fit. Academy of Management Review, 14: 333-349.

Checkland, P.B. & Scholes, J., 1990 Soft Systems Methodology in Action.John Wiley, Chichester, UK.

Choi, S. Y., Lee, H., & Yoo, Y. 2010. The Impact of Information Technology and Transactive Memory Systems on Knowledge Sharing, Application, and Team Performance: A Field Study. MIS quarterly, 34(4), 855-870.

Clemen, R.T., 1996 Making Hard Decisions. Duxbury, Belmont, CA, USA.

Coles, R.S. & Moulton, R., 2003 Operationalizing IT risk management. Computers and Security, 22, 487–493.

Daniels, K., de Chernatony, L. & Johnson, G., 1995 Validating a method for mapping manager's mental models of competitive industry structures. Human Relations, 48, 975–991.

Daulatran BL, 2003 Organizational Culture and Job Satisfaction. Journal of Business and Industrial Marketing, 18(3):225.

Deal, T.E. & Kennedy, A.A. 1982, Organization Cultures: The Rites and Rituals of Organization Life, Addison-Wesley.

Dhillon, G., 1997 Managing Information System Security. Macmillan, London, UK.

Dhillon, G., 2001 Violation of safeguards by trusted personnel and understanding related information security concerns. Computers and Security, 20, 165–172.

Dhillon, G., & Torkzadeh, G. 2006. Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314.

Drevin, L., Kruger, H.A. &Steyn, T., 2007 Value-focused assessment of ICT security awareness in an academic environment'.Computers and Security, 26(1).p36-43.

Emory, C.W. & Cooper, D.R., 1991 Business Research Methods.Irwin, Boston, MA, USA.

Gibson, Q., 1960 The Logic of Social Inquiry. Routledge, London, UK.

Giddens, A., 1984 The Constitution of Society. Polity Press, Cambridge, UK.

Hitchings, J., 1996 A practical solution to the complex human issues of information security design. In: Information Systems Security: Facing the Information

Society of the 21st Century, Katsikas, S.K. &Gritzalis, D. (eds), pp. 3–12. Chapman & Hall, London, UK.

Holden, R. J., & Karsh, B. T. 2010. The technology acceptance model: its past and its future in health care. Journal of biomedical informatics, 43(1), 159-172.

Humaidi, N., & Balakrishnan, V. 2013. Exploratory Factor Analysis of User's Compliance Behaviour towards Health Information System's Security. Journal of Health & Medical Informatics.

Hunter, M.G., 1997 The use of RepGrids to gather datanabout information systems analysts. nformation Systems Journal, 7, 67–81.

Karyda, M., Kokolakis, S. &Kiountouzis, E., 2003 Content, context, process analysis of IS security policy formulation. In: Security and Privacy in the Age of Uncertainty, Gritzalis, D., Vimercati, S.D.C., Samarati, P. &Katsikas, S. (eds), pp. 145–156. Kluwer Academic Publishers, Boston, MA, USA.

Keeney, R.L., 1999 The value of internet commerce to the customer. Management Science, 45, 533–542.

Keeney, R.L., 1994 Creativity in decision making with value-focused thinking. Sloan Management Review, 35, 33–41.

Keeney, R. L., & Keeney, R. L. 2009. Value-focused thinking: A path to creative decisionmaking. Harvard University Press.

Kreicberge, L. 2010. Internal threat to information security countermeasures and human factor with SME. Business Aministration and Social Sciences. Lulea University of Technology, 1-66.

Leach, J. 2003. Improving user security behaviour. Computers & Security,22(8), 685-692.

Ling, A. P. A., & Masao, M. 2011, May. Selection of model in developing information security criteria on smart grid security system. In Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on (pp. 91-98). IEEE.

Maier, R., & Hädrich, T. 2011. Knowledge Management Systems.

Nah FF, Siau K, Sheng H., 2005 The value of mobile applications: a utility company study. Communications of the ACM; 48(2):85–90.

Orlikowski, W.J., 1993 CASE tools as organizational change: investigating incremental and radical changes in systems development. MIS Quarterly, 17, 309–340.

Orlikowski, W.J. & Gash, D.C., 1994 Technological frames: making sense of information technology in organizations. ACM Transactions on Information Systems, 12, 174–207.

Orlikowski, W.J. &Robey, D., 1991 Information technology and structuring of organizations. Information Systems Research, 2, 143–169.

Pfleeger CP, Pfleeger SL., 2003 Security in computing. 3rd ed. Prentice Hall.

Phythian, G.J. & King, M., 1992 Developing an Expert System for tender enquiry evaluation: a case study. European Journal of Operational Research, 56, 15–29.

Popova, V., & Sharpanskykh, A. 2010. Modeling organizational performance indicators. Information Systems, 35(4), 505-527.)

Posner, Barry Z, Kouzes, J.M., and Schimdt, W. H., 1985, Shared Values Make a Difference: An empirical test of corporate culture. Human Factorss Management, 24(3): 293-310.

Saeed Soltanmohammadi, Saman Asadi, Norafida Ithnin, Dr. 2013, main human factors affecting information system security. November edition Volume 5, number 7.

Samy NG, Ahmad R, Ismail Z 2010 Security threats categories in healthcare information systems. Health Informatics J 16: 201-209.

Segev, A., Porra, J. &Roldan, M., 1998, Internet security and the case of Bank of America. Communications of the ACM, 41, 81–87.

Shaw, M.L.G., 1980 On Becoming a Personal Scientist: Interactive Computer Elicitation of Personal Models of the World. Academic Press, New York, NY, USA.

Siponen, M., Pahnila, S., & Mahmood, M. A. 2010. Compliance with information security policies: An empirical investigation. Computer, 43(2), 64-71.

Simpson, B. & Wilson, M., 1999 Shared cognition: mapping commonality and individuality. Advances in Qualitative Organizational Research, 2, 73–96.

Simpson, B. & Wilson, M., 1999 Shared cognition: mapping commonality and individuality. Advances in Qualitative Organizational Research, 2, 73–96.

Siponen, M.T., 2001 An analysis of the recent IS security development approaches: descriptive and prescriptive implications. In: Information Security Management: Global Challenges in the New Millennium, Dhillon, G. (ed.), pp. 101–124. Idea Group Publishing, Hershey, PA, USA.

Smart, D. T., & Conant, J. S. 2011. Entrepreneurial orientation, distinctive marketing competencies and organizational performance. Journal of Applied Business Research (JABR), 10(3), 28-38.

Spender, J.C., 1998 The dynamics of individual and organizational knowledge. In: Managerial and Organizational Cognition, Eden, C. & Spender, J.C. (eds), pp. 13–39. Sage, London, UK.

Stamp, M. 2011. Information security: principles and practice. John Wiley & Sons.

Straub, D.W. &Welke, R.J., 1998 Coping with systems risks: security planning models for management decision making. MIS Quarterly, 22, 441–469.

Tan, F.B. & Hunter, M.G., 2002 The repertory grid technique: a method for the study of cognition in information systems. MIS Quarterly, 26, 39–57.

Torkzadeh, G. &Dhillon, G., 2002 Measuring factors that influence the success of internet commerce. Information Systems Research, 13, 187–204.

Trompeter, C.M. &Eloff, J.H.P., 2001 A framework for implementation of socio-ethical controls in information security. Computers and Security, 20, 384–391.

Venkatesh, V., & Davis, F. D. 2000. A theoretical extension of the technology acceptance model: four longitudinal field studies. Management science, 46(2), 186-204.

Wakhlu, Bharat, 1986 The importance of Value in Organizations, Management and Labor Studies, Vol: 11: 262-265.

Walker, R. M., Damanpour, F., & Devece, C. A. 2011. Management innovation and organizational performance: the mediating effect of performance management. Journal of Public Administration Research and Theory, 21(2), 367-386.

Weick, K.E., 1995 Sensemaking in Organizations. Sage Publications, Beverly Hills, CA, USA.

Weick, K.E. &Bougon, M.G., 2001 Organizations as cognitive maps: charting ways of success and failure. In: Making Sense of the Organization, Weick, K.E. (ed.), pp.308–329. Blackwell Publishers, Malden, MA, USA.

Wheeler, B.C., 2002 NEBIC: a dynamic capabilities theory for assessing net-enablement. Information Systems Research, 13, 125–146.

Whitman ME, Mattord HJ., 2005 Principles of information security.2nd ed. Thomson.

Willcocks, L. &Margetts, H., 1994 Risk assessment and information systems. European Journal of Information Systems, 3, 127–139.

Wing, J.M., 1998 A symbiotic relationship between formal methods and security. Proceedings from Workshops on Computer Security, Fault Tolerance, and Software Assurance: from Needs to Solution. CMU-CS-98-188, December.

Zeleny, M., 1982 Multiple Criteria Decision Making.McGraw-Hill, New York, NY, USA.

Zhu, D., Premkumar, G., Zhang, X. & Chu, C., 2001 Data mining for network Intrusion Detection: a comparison of alternative methods. Decision Sciences, 32, 1–26.