IMPROVING INFORMATION SYSTEM SECURITY BY EVALUATING HUMAN FACTORS

SAEED SOLTANMOHAMMADI

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master Computer Science

Faculty of Computing
Universiti Teknologi Malaysia

August 2013

I dedicated this thesis to my beloved mother, and father for their endless supports and encouragements.

ACKNOWLEDGEMENT

IN THE NAME OF GOD, MOST GRACIOUS, MOST COMPASSIONATE

I would like to acknowledge my supervisor, **Dr. NORAFIDA ITHNIN**, for her support, encouragement, guidance, astute and expert editing. I would like to express gratitude for his patience, generosity, and collaboration.

My lovely family; thank you for your perpetual encouragement and support. Your unwavering love that have shaped my mind and opened the doors of opportunity leading me to become the person I am today.

I would like to thank all of the individuals who have helped me during my thesis study.

ABSTRACT

Health Information System (HIS) has been implemented in Malaysia since late 1990s. HIS is an integration of several hospitals' information system to manage administration works, patients and clinical records. Accessing HIS data through the internet make it more vulnerable to data lost, misuses and attacks. Health data is extremely sensitive, therefore they require high protection and information security must be carefully watched as it plays an important role to protect the data from being stolen or harmed. Despite the vast research in information security, the human factor has been neglected from the research community, with most security research giving focus on the technological component of an information technology system. The human factor is still subject to attacks and thus, in need of auditing and addressing any existing vulnerabilities. This research evaluates the human factor by the creation of a survey which examines three distinct user properties. Each of these properties comprises a series of questions, which with their turn assist on confirmation or refutation of three hypotheses. The survey was conducted on five public and private hospitals in Malaysia and distributed to all members of staff who have access on electronic information. Results have shown that the human factor has a significant role in information security; among the surveyed factors (organizational factor, motivational factor and learning), it is confirmed that Learning has the most effect on information system security. This research has addressed two sub factors of learning that are organizational learning and individual learning. In order to improve the information system security in hospitals, it is recommended for future study to consider some other factors except these two sub factors in learning.

ABSTRAK

Sistem Maklumat Kesihatan (HIS) telah dilaksanakan di Malaysia sejak 1990-an. HIS adalah integrasi sistem maklumat beberapa hospital untuk pengurusan kerja-kerja pentadbiran, pesakit dan rekod klinikal. Pengaksesan data HIS melalui Internet menjadikan ia lebih terdedah kepada risiko kehilangan data, penyalahgunaan dan serangan. Data kesihatan adalah sangat sensitif, oleh itu mereka memerlukan perlindungan yang tinggi dan keselamatan maklumat yang perlu pengawasan yang tinggi kerana ia memainkan peranan yang penting untuk melindungi data daripada dicuri atau dirosakkan. Walaupun penyelidikan yang luas dalam Keselamatan Maklumat, faktor manusia telah diabaikan daripada komuniti penyelidikan, dengan kebanyakan penyelidikan keselamatan memberi tumpuan kepada komponen teknologi sistem Teknologi Maklumat. Faktor manusia adalah masih tertakluk kepada serangan dan dengan itu, memerlukan pengauditan dan menangani sebarang kelemahan yang sedia ada. Kajian ini menilai faktor manusia dengan mewujudkan satu kajian yang mengkaji tiga sifat pengguna yang berbeza. Setiap satu daripada sifat-sifat ini terdiri daripada beberapa soalan, yang dengan giliran mereka membantu dalam pengesahan atau penyangkalan tiga hipotesis. Kaji selidik itu dijalankan di lima hospital awam dan swasta di Malaysia dan diedarkan kepada semua kakitangan yang mempunyai akses kepada maklumat elektronik. Keputusan telah menunjukkan bahawa faktor manusia mempunyai peranan penting dalam Keselamatan Maklumat; antara faktor yang dikaji (Faktor Organisasi, Faktor Motivasi dan Pembelajaran), ia mengesahkan bahawa Pembelajaran mempunyai kesan yang paling atas Sistem Maklumat Keselamatan. Kajian ini telah ditangani dua faktor sub Pengajian yang Pembelajaran Organisasi dan Pembelajaran individu. Dalam usaha untuk meningkatkan Sistem Keselamatan Maklumat di hospital-hospital, ia adalah disyorkan untuk kajian masa depan untuk mempertimbangkan beberapa faktor-faktor lain kecuali kedua-dua faktor sub dalam Pembelajaran.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

With less concern for people and organizational issues, a major part of information systems security strategies are technical in nature. As a consequence, since most information systems security strategies are of importance as they concentrate on technical oriented solutions, for instance checklists, risk analysis and assessment techniques, there is a necessity to investigate other ways of managing information systems security as they tend to disregard the social factors of risks and the informal structures of organizations.

This investigation concentrates chiefly on human and organizational factors within the computer and information security system. The impact on security can be drastic if human and organizational factors influence their employment and use, irrespective of the power of technical controls (Bishop, 2002). In this aspect, the juncture for computer and information security vulnerabilities may be set by vulnerable computer and information security protection (e.g., weak passwords or poor usability) and malicious intentions may appear. The results of blemished organizational policies and individual practices whose origins are deeply rooted within early design presumptions or managerial choices causes susceptibilities (Besnard and Arief, 2004).

1.2 Background of the Study

The protection of the confidentiality, integrity and access to information is referred to as information security (Kruger and Kearney, 2006). Evidence indicates that, organizations will still undergo security breaches in spite of the amount of technical controls in position (Schultz, 2005; Besnard andArief, 2004). Indeed, the 2007 CSI Computer Crime and Security Survey reported that 52% were still plagued with viruses although 98% of users possess anti-virus software (Richardson, 2007). This is due to information security not only being a technical problem but a 'people' problem as well (Schulz, 2005). It is, nevertheless, important to state that virus infections will not be fully safe-proof even with anti-virus software that is ideally used, which suggests that this is not just a 'people' problem, but a technical problem as well. In spite of this, employees' inability to conform to information security guidelines is the reason for most of the breaches in information security, as some evidence suggests (Chan *et al.,*2005). In backing this finding, information security experts who were quizzed, by which results of the 2007 Global Security Survey were based on, showed that 79% of respondents believe human error to be the source of failures in information systems (Deloitte, 2007).

Everyone is aware that the key to the central information security issue is changing the way people – regular people, not computer scientists or engineers – perceive about what security is: end users may not act on these issues in spite of them being aware of those issues. This means the use of security technology will continue to be sub-ideal regardless of how good the technology of security is. The analysis of human factors on security acquiescence has remained mostly disregarded in Information Security (INFOSec) and Information Assurance literature in spite of the fact that non-technical computer users are the weak connection in information systems security. An implied presumption seems to be that adequate technology will overcome the issue – meaning, we can automate our way to information systems security if only we are able to take out humans from the equation. The presumption that technology will overcome the security issue has yet to be proven and, while not denying the fact that technology is definitely vital, but, in reality, is rebutted by the

HCI expert, Jacob Nielsen. Moreover, it overlooks the general aphorism that security has three portions: technology, process and people.

1.3 Statement of the Problem

It is an incorrect presumption that system security expectations should be realized when people follow by avoiding secure behavioral outlines. Security is something that can be easily purchased is another incorrect allegation; that human factor can sometimes demonstrate the most reliable expectations, incorrect. A critical point in Information Security is without question the human factor. An attacker would take advantage of people who might make untried decisions which would permit, or might even purposely attack their premises.

Since numerous organizations use and apply advanced technologies in their security systems such as smart card and biometrics, external threats are not the main concerns in information security (Kreicberge, 2010 and Leach, 2003). As Leach (2003) stated, the main concerns are related to internal threats such as users' carelessness, errors and omissions which are all caused by internal factors an categorized as poor users' behaviors. 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, and Balakrishnan, 2013).

1.4 Objectives of the Study

1. To identify the Human Factors that affect Information System Security based on previous studies.
2. To propose a new framework for Health Information System Security.
3. To assess the proposed framework in Malaysian hospitals.

1.5 Significant of the Study

Health Information System has been applied in Malaysia since late 1990s. Now Health Information System is used in numerous government and private hospitals. Health Information System is a combination of some hospitals' information system to control administration tasks, patients and clinical evidences. It is possible to access Health Information System via Internet and the data can be delivered, saved and processed automatically. Moreover, the system is available through Internet which means that the system is at risk to improper use (Humaidi and Balakrishnan, 2013). Health data is too sensitive, hence they need high protection and information security must \ protect the data cautiously from being stolen or harmed.

The human factor has been discovered to want interest from the research fraternity in spite of the extensive study in Information Security, with most security investigations concentrating on the technological constituent of an Information Technology system. The human factor is still prone to attacks notwithstanding any technological solutions presented, and hence, in need of auditing and highlighting any present vulnerabilities.

Considering the points mentioned above, results of this study will help healthcare industry of Malaysia in order to decreasing the Human Errors. In addition, this study develops a new Framework that categorizes the Human Factors to three groups: Organizational Factors, Motivational Factors and Learning.

1.6 Scope of the Study

The scope of this study is health care industry of Malaysia. For this purpose Malaysian hospitals are considered as a target. These hospitals are located in KL, Serdang and Johor.

1.7 Organization of Remaining Chapters

This study consists of six chapters. In chapter one, overview, problem statement, objectives and also significance of study are presented. The rest part of this study has the following structure:

Chapter 2 – Literature Review: This chapter attempts to provide necessary concepts and issues that lead to better understanding of purpose of this study. Definitions of Information System Security, System Security Goals, System Security Threats, Human Error, Rule of Human Factor in Information System Security, and based on literature will highlight the independent and dependent variables.

Chapter 3 – Hypothesis Developing and Methodology: This chapter attempts to generate an appropriate conceptual frame work for this study to explain the relationship between the variables (independent and dependent). For this purpose all variables are justified based on literature and current conditions. Besides, it describes method of data collecting, screening and analyzing.

Chapter 4 – Data Analysis: This chapter covers the quantitative analysis, research design and the suitable methodology in relation to impact of mentioned independent variables on Information System Security. Besides, it explains the sample of study, data collection, different variables for developed model, and the statistical tool applied in this research. Thus, the result will provide in terms of descriptive statistics, and Regression analysis.

Chapter 5 – Discussion and Conclusion: Chapter five discusses results, and answers to all research questions based on analyzed data. In addition, after limitation of study section, some relevant topics in term of Information System Security will be suggested.

Chapter 6 –Recommendation and Future Study: Regarding to the final result, some guidelines for improving Information System Security and also some topics for further research study would be recommended.

REFERENCES

Aarons GA (2006) Transformational and transactional leadership: Association with attitudes toward evidence-based practice. PsychiatrServ 57: 1162 1169.

Adams, A. Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 41-46.

Ahmed, M., Sharif, L., Kabir, M., Al-Maimani, M. (2012).Human Errors in Information Security. International Journal, 1(3).

Albrechtsen, E. (2007). A qualitative study of users' view on information security.Computers & Security, 26(4), 276–89.

Anderson, R. J. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems (2nd ed.). New York: Wiley.

Arce, I. (2003). The weakest link revisited, IEEE Security and Privacy, 1,72–76.

Bass BM (1985) Leadership and performance beyond expectation.The Free Press, New York.

Besnard, D. Arief, B. (2004).Computer security impaired by legitimate users. Computers and Security, 23, 253-264.

Bishop, M. (2002). Computer security: art and science. Addison Wesley Professional.

Bishop, M. (2003). Computer Security: Art and Science. Pearson Education, Inc.

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.

Brostoff, A. (2004). Improving password systems effectiveness, PhD thesis, UCL, UK, unpublished.

Bubb, H. (2005). Human reliability: a key to improved quality in manufacturing, Human Factors and Ergonomics in Manufacturing, 15(4), pp.353–368, Wiley Periodical.

Burns JM (1978) Leadership, Harper and Row , New York.

Carayon, P., Kraemer, S. (2009). A human factors vulnerability evaluation method for computer and information security.

Chan, M., Woon, I. &Kankanhalli, A. (2005). Perceptions of information security at the workplace: Linking information security climate to compliant behavior, Journal of Information Privacy and Security, 1(3), 18-42.

Cresswell, A.,Hassan, S. (2007). Organizational impacts of cyber security provisions: a sociotechnical framework. In: 40th Hawaii International Conference on Systems Sciences.

Danchev, D. (2006). Reducing ”human factor” mistakes.

Deloitte (2007). 2007 Global Security Survey: The Shifting Security Paradigm. Deloitte Touche Tohmatsu.

Dhillon G., Backhouse J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11:127–53.

Edwards, C., Kharif, O., and Riley, M. (2011). Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy, Bloomberg, June 2011. Online at http://www.bloomberg.com/news/2011- 06-27/human-errors-fuel-hacking-as-test-showsnothing- prevents-idiocy.html.Accessed on 13th March 2012.

Embrey, D. (2005). Understanding human behaviour and error. Human Reliability Associates, 1, 1-10.

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. In Proceedings of the Human Factors Society 32nd Annual Meeting (pp. 97-101). Santa Monica, CA: Human Factors Society.

Fiol, C. M., & Lyles, M. A. (1985).Organizational learning. Academy of Management review, 10(4), 803-813.

Fischer Russell Sage Foundation. 2011. 176 pages. $24.95 paper. Social Forces.Still Connected: Family and Friends in America Since 1970 By Claude S.

Fischer-Hübner, S. (2001). IT-security and privacy: design and use of privacy-enhancing security mechanisms. Springer-Verlag.

Flechais, I. (2005). Designing Secure and Usable Systems, University College London.

Fotta, M. E., Byrne, M. D., & Luther, M. S. (2005). Developing a human error modeling architecture (HEMA). Proceedings of Human-Computer International, Mahwah, NJ, USA. Lawrence Erlbaum Associates, Inc.

Fujita Y, Hollnagel E. (2004). Failures without errors: quantification of context in HRA. ReliabEngSyst Safety, 83:145–51.

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), 106–14.

Furnell S. (2007). Making security usable: are things improving? Computers & Security, 26(6):434–43.

Furnell, S. (2005). Why users cannot use security. Computers and Security, 24, 274 279.

Gonzales, J. J. &Sawicka, A. (2002). A Framework for Human Factors in Information Security, Proceedings of the WEAS International Conference on Information Security, Rio de Janeiro, Brazil.

Gonzalez, J. J., Sawicka, A. (2003). A framework for human factors in information security.

Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., and Williams, T. (2011).Gray Hat Hacking, The Ethical Hacker's Handbook, Third Edition, McGraw Hill.

Hassell, L. &Wiedenbeck, S. (2004). Human Factors and Information Security, Drexel University College of Information Science and Technology.

He, X., Wang, Y., Shen, Z., & Huang, X. (2008).A simplified CREAM prospective quantification process and its application. Reliability Engineering & System Safety, 93(2), 298-306.

Hinson, G. (2003). Human factors in information security.

Hollnagel E. (1998). Cognitive reliability and error analysis method. Oxford, UK: Elsevier Science Ltd.

Hollnagel, E. (1993). Human Reliability Analysis: Context and Control, London: Academic Press.

Hu D, Xu W, Shen H, Li M (2005) Study on information system of health care services management in hospital. Services Systems and Services Management, Proceedings of ICSSSM '05. 2005 International Conference.

Huang, D., Rau, P.P. &Salvendy, G. (2007).A survey of factors influencing people's perception of information security.In J. Jacko (Ed.).Human-Computer Interaction, Part IV. Heidelberg: Springer.

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

Jensen, R. S. (1982). Pilot judgment training and evaluation.Human Factors, 24(1), 61- 73.

Kahraman, E. (2005). Evaluating it security performance with quantifiable metrics.Master's thesis, DSV SU/KTH.

Karyda, M., Kiountouzis, E., Kokolakis, S. (2005). Information systems security policies: a contextual perspective. Computers & Security, 24, 246–60.

Kaushal, S (2011) Effect of leadership and organizational culture on information technology effectiveness: A review. Research and Innovation in Information Systems (ICRIIS) International Conference.

Keep, E. (2000).Learning organisations, lifelong learning and the mystery of the vanishing employers. Economic Outlook, 24(4), 18-26.

Koskosas I, Kakoulidis K, Siomos C (2011) Examining the linkage between information security and end-user trust. International Journal of Computer Science & Information Security 9: 21-31.

Kraemer, S., Carayon, C., Clem, J. F. (2006).Characterizing violations in computer and information security systems. In: Proceedings of the 16th triennial congress of the international ergonomics association. Maastricht, The Netherlands.

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), 143–54.

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.

Kruger, H. A. & Kearney, W. D. (2006).A prototype for assessing information security awareness. Computers and Security, 25, 289-296.

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

Lo M-C, Ramayah T, de Run EC (2010) Does transformational leadership style foster commitment to change? The case of higher education in Malaysia.ProcediaSocBehavSci 2: 5384-5388.

Maiwald, E. (2004). Fundamentals of Network Security.McGraw-Hill Technology Education.

Martin N, Rice J (2011) Cybercrime: Understanding and addressing the concerns of stakeholders. Computers & Security 30: 803-814.

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

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

Newman, R. E. (2003). Enterprise Security, Pearson Education, Inc., first edition.

Nikolakopoulos, T. (2009).Evaluating the human factor in Information Security.

Norman, D. A. (1981). Categorization of action slips. Psychological Review, 88(1), 1-15.

Nunnally, J. (1978). Psychometric methods. McGraw-Hill, New York, NY.

Pahnila, S., Siponen, M., Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), IEEE.

Pfleeger, C. P., &Pfleeger, S. L. (2003). Security in computing.Prentice Hall.

Pickard, A. J. (2007) .Research Methods in Information.Facet Publishing.

Raymond, R. P. (2004). Corporate Computer and Network Security, Pearson Education, Inc.

Reason, J. (1990). Human Error, Cambridge, UK: Cambridge University Press.

Reason, J. (1997).Managing the Risks of Organizational Accidents.Ashgate, Brookfield.

Reason, P., Rowan, J.v(1981). Human inquiry: a sourcebook of new paradigm research, Chichester: John Wiley.

Richardson, R. (2007). 2007 CSI Computer Crime and Security Survey. Computer Security Institute.

Roberts, P. (2004). AOL survey finds home user ignorant to online threats, ComputerWeekly, April 2010. Online at http://www.computerweekly.com/news/2240058434/AOLsurvey- finds-home-user-ignorant-to-online-threats.Accessed on 10th March 2012.

Ruighaver, A. B., Maynard, S. B., Chang, S. (2007). Organisational security culture: extending the end-user perspective. Computers & Security, 26(1), 56–62.

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.

Salkind, N. J (2003).Exploring Research. Pearson Education, Inc., fifth edition.

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

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

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.

Sasse, M. A., Brostoff, S. &Weirich, D. (2001).Transforming the 'weakest link' – a human/computer interaction approach to useable and effective security. BT Technology Journal, 19(3), 122-131.

Schneier, B. (2000). Secrets and Lies. Robert Ipsen.

Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World, Indianapolis, IN: Wiley Publishing, Inc.

Schultz, E. (2005). The human factor in security. Computers & Security, 24:425–426.

Schultz, E. (2005). The human factor in security. Computers and Security, 24, 425-426.

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

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

Spruit, M. E. M., Looijen, M. I. T. (1996). security in Dutch practice, Computers and Security, 15(2), pp. 157–170.

Stanton, J. M., Stam, K. R., Mastrangelo, P., Jeffery, J. (2005). Analysis of end user security behaviors, Computers & Security, 24, 124–33.

Swain, A. D., &Guttman, H. E. (1983).Handbook of human reliability analysis with emphasis on nuclear power plant applications.NUREG/CR-1278, U.S. Nuclear Regulatory Commission, (Washington D.C.).

Wagner, D. A., Crabb, M. D. (1997). System security: A management perspective, September.

Werlinger, R., Hawkey, K., Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security, 17(1), 4–49.

William, L. S., Kevin, D. M. (2002).The Art of Deception.Wiley Publishing, Inc.