INFORMATION SECURITY AWARENESS AMONG SYSTEM ADMINISTRATORS AND END-USER PERSPECTIVES

PUGNESWARY A/P PANNER SELVAN

UNIVERSITI TEKNOLOGI MALAYSIA

INFORMATION SECURITY AWARENESS AMONG SYSTEM ADMINISTRATORS AND END-USER PERSPECTIVES

PUGNESWARY A/P PANNER SELVAN

A dissertation submitted in partial fulfilment of the
requirement for the award of the degree of
Master of Science (Information Technology Management)

Advanced Informatics School
Universiti Teknologi Malaysia

NOVEMBER 2016

Special Thanks:

This dissertation is dedicated to my beloved family, friends and lecturers who never fail to encourage me along my journey.

ACKNOWLEDGEMENT

The completion of this dissertation would not have been possible without the support of people around me. I would like to thank my supervisor Dr. Roslina Ibrahim for her support and valuable advice throughout my dissertation. The feedback she provided during our regular meetings helped me in accomplish my dissertation. I would like to acknowledge my family for their continuous encouragement throughout my studies. Without my colleagues participation this research would not have been possible. Thank you for the expertise and knowledge which helped improves my work. Also my beloved friends' thank you for the encouragement and helpful support that inspired me to pursue this route. Above all, I give honor and praise to Lord for giving me strength and his guidance throughout my studies.

ABSTRACT

Information security breaches is a current serious issue that has been faced by many organizations. Many ways have been discovered to reduce the number of security breaches such as technical and non-technical methods. Yet the issue still occurs because of the humans unconcerned behaviors. The results of this dissertation have increased the understanding the fact that human factor is the main cause in the information security vulnerabilities in an organization. The objective of this dissertation is to project the information of the security practices and the awareness level among the system administrator and end user at the same time to proof that the human error is the major factor for the security breaches. The research demonstrated the type of breaches, rate and education that can be given to the employee on how to reduce the security breaches during their daily task performance. Questionnaires for the end users, discussion sessions with the system administrators and data collections from archival records have supported the dissertation. Based on the analysis, the end users created threats due to many factors such as user skills or capabilities and users' attitude towards the technological tools or introduction to new process in the organization. Data were analyzed using Statistical Package for the Social Science (SPSS) quantitative data analysis. The findings from surveys collection and interviews sessions showed that the end users need more education on self-awareness against security attacks around them while the system administrator should always be ready to support the security awareness level and help to educate the awareness among the employee in the organization.

ABSTRAK

Banyak cara telah ditemui untuk menangani isu keselamatan data di sesebuah organisasi. Kaedah teknikal seperti pemasangan alat pengawasan pengunaan internet dan kaedah bukan teknikal seperti mendidik kakitangan supaya lebih celik dengan isu keselamatan data semasa. Kajian ini lebih tertumpu kepada pendekatan bukan teknikal yang menganalisis tahap amalan dan kesedaran keselamatan data di kalangan pentadbir system maklumat dan kakitangan dalam sesebuah organisasi. Soal selidik, sesi perbincangan dengan pentadbir system maklumat dan rekod arkib dari organisasi telah membantu dalam pengumpulan data untuk tujuan kajian ini. Berdasarkan analisis, keputusan menunjukkan bahawa pentadbir sistem maklumat mempunyai lebih perhatian terhadap kecuaian kakitangan yang disebabkan oleh pelbagai faktor seperti kemahiran, keupayaan dan sikap kakitangan dalam penggunaan alat teknologi dan sikap cuai atau pentingkan komplitasi kerja harian. Kajian ini juga diplotkan terutamanya untuk kakitangan berkongsi perspektif mereka mengenai ancaman keselamatan sistem maklumat di dalam sesebuah organisasi. Data dianalisis dijalankan dengan penggunaan Pakej Statistik untuk Sains Sosial (SPSS) bagi menganalisis data kuantitatif dari kajian ini. Hasil kajian ini telah meningkatkan pemahaman tentang hakikat bahawa faktor manusia adalah punca utama dalam kelemahan keselamatan maklumat dalam sesebuah organisasi. Kakitangan perlu diberikan perhatian yang lebih dalam mendidik mereka untuk kesedaran diri terhadap serangan keselamatan maklumat dari sekeliling mereka.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.0 Introduction

Information is the crown jewels for most of the business assets nowadays. It is important to an organization's business and needs to be properly protected where business environment are now depends on the technologies. As a result of this interconnectivity ramble, "information is also exposed to a growing number of threats and vulnerabilities" (ISO 27001:2005, 2008). For this reason, many organizations now are trying to implement various security policies, governance or security awareness programs within the organization in order to protect their information. According to recent research, around 60 percent of information securities incidents are caused by human error and the second highest are by malicious activity from hackers and scammers.

These kinds off careless mistakes have real costs and consequences for the organizations and clients. Organizations has experienced an average of 122 successful attacks every week and up from 102 attacks per week in 2012. Information security management systems have increasingly become important for all sectors across all business environments. Information technology systems are used in a variety of ways including data processing, data transmission, storage, and technology backups.

The protection of these information systems from different security attacks is a constant challenge for the security team in an organization. Companies spend high in cost in order to ensure that their information systems are both protected from security threats and compliance with organization's policy. A recent researched conducted by the Phenomenon Institute and sponsored by HP Enterprise Security Products reflected the 2013 Cost of Cyber Crime results.

It tosses around some eye-catching numbers which is the average cost of cybercrime experienced by a benchmark sample of US organizations was $11.56 million, with a range of $1.3 to $58 million. That represents 78 percent increase from the initial research which was conducted four years ago" (Symantec and the Phenomenon Institute, 2013). Both the efforts in protecting the data and the challenge grows together due to the fact that the types of threats change at the same pace with the technology advances.

The protection of data becomes even more difficult for multinational companies where the nature of the business commands a diverge level of authority, accessibility and availability in both software and hardware to meet their business objectives. "(Victoria Mahabi, 2010, (Hasan & Yurcik, 2008-2010)) has analyzed that 35 percent out of 219 which was the largest portion of the reported breaches were reported by the global institutions from the year 2008 to 2010."

The client will always want to know if we have done sufficient enough to protect their information assets during the business periods. The key component that drives the business is definitely the information and most business cannot function if this element is unreliable. In today's high technology world, availability, integrity and confidentiality of information are the greatest concerns of today's world where all the records are kept in computers and accessible from anywhere, via the Internet.

We can never be sure that all our information is secure and confidential all the time in this digitized world. “All the global organizations are constantly challenged in achieving their business and technology objectives to provide true-value to their stakeholders” (Raees Khan, 2010 (COBIT, 2005)). Essentially, these leading global organizations are increasingly rely on a variety of information assets, such as skilled personnel, complex business processes and the latest technology to perform various functions across all business units.

One of the most compelling challenges encountered by the organizations is the lack of clear view on the organizational information security structures and the awareness level. The convergence of global connectivity and the critical dependence on technology to run an organization, is leading a way together increasing the professional threats and organized cybercrime.

Present-day security for information systems are vulnerable to a host of threats by cyber-terrorists or hackers, such as virus spreading through the Internet, social engineering attacks or the inappropriate use of the Net's assets. The permanent nature of security threats and complexity of IT infrastructures are currently leading organizations throughout the world to revise their approaches in information security.

The organizations fully recognize the need to continuously improve their internal security values by establishing and maintaining a proper security processes and procedures. Some organizations are still relying on outdated security standards, such as the ISO/IEC 17799, which were developed when current ICT threats and complexities were still unheard off.

The most recent ISO/IEC 27001:2013 standard has finally introduced the notion of a security policy life-cycle but in today's dynamic ICT environments, emerging threats and sudden changes in technology may require much more responsive decision-making procedures. It clearly shows that information security is very important to provide the much needed safety to the information.

There are two main reasons for security should be implemented and viewed as important assets for everyone. First, personal protection of information and secondly is the social security thru network where connection from PC to the external networks that connected to outside social communities. E.g. A network trespasser will connect to the external networks to gain access by launching a platform to attack other machines.

It is very common for network trespassers to take control of server machines and route the traffic to make a trace back more difficult. There are many other exposures that are often found on systems or websites in an organization such as denial of service attack, unavailability of firewall, buffer overflow, threats from viruses, hackers and spam, and many other security defects.

Due to these kinds of security attacks, it has become very important for organizations to assess their security requirements of all their assets which include the hardware and software assets. Securing information systems can be achieved by using both technical and non-technical methods. Technical methods apply cryptography, strong authentication methods or security physical models.

Non-technical approaches focus on improving users' behaviors, educating and train the users, and secure usage of IT systems by encouraging a standard tools or platforms in an organization. System administrator and end users' perspective will be target to evaluate the information security practices and level of user awareness to find out how the security steering functions and supports awareness programs and respond to user behaviors that pose the highest risks to the systems in their daily activities.

1.1 Background of the Problem

Over the last 10 years, the usage of information system in the enterprise level has exploded. That explosion of technology may do wonders for production, but it can give IT and security professionals challenges to deal with unauthorized usage, and also in safeguarding against the loss of the information. In this new harden environment, security solutions in protecting its physical infrastructure, applications and data accessible through the Internet or intranets from threats is getting tougher.

Protecting information has become a critical task of all organizations in their daily business activities. This reality is even more pressing in companies which information is part of their core business. “In fact, in last few years, we have observed increasingly organizations becoming heavily dependent on technology and therefore undoubtedly at the heart of critical infrastructures” (Daniel Mellado, David G.Rosado, 2012 (Blanco et al, 2010)).

“Furthermore, the current trend towards using information systems are bigger and well distributed throughout the entire Internet which has led to the rise of new challenges to security professionals” (Daniel Mellado, David G.Rosado, (Opdahl and Sindre, 2008). Information security awareness trainings or policy implementation often fails to teach the users on their contribution towards the improvement of the organization’s information security.

56 percent of system administrator claimed that they train the end users during the new joiner orientation while only 32 percent of employees admitted that they have been educated on enterprise information security policy. This gap has resulted serious problems where research shows that 14.4 percent of data loss incidents per year due to employee negligence and 15 percent of them have reported an insider breaches executed with malicious intention.

Technologies that are sneaking into the workplace to maintain the information security isn't just an issue but also the end users who are not obeying on the security practices. These actions will also affect the security professionals where disagreement appears between the system administrator and the end users solely because the security department will point out the mistakes that occur rather than solving the issues on the business needs.

Technologies have created new challenges for the security systems which not only depend on the technical assets for solutions, but also on people's ability to understand and use the assets as part on their daily business. As a step towards solving this problem, we have been examining on how people dealing with the information security threats in their daily life.

1.2 Problem Statement

Given the current scenario in the entire challenging technology world, the situation clearly shows that security is very important to provide safety to the user's privacy and information. Lack of security awareness includes viruses, phishing, stolen passwords or social engineering is very harmful to the daily operation of an organization. It is expected that organizations with least security awareness programs will have high security breaches caused by the employees. Past researches and data show that, many organizations have not been able to reduce security issues.

Therefore, it is important to conduct further research on this case for a better understanding on the factors involved, applied approaches and effectiveness of these approaches to create awareness on the human ethical towards information security. Comparison on the perception among the end users and system administrators is also important. System administrators may operate under the assumption that IT policies are clearly understood by the employee before authorizing the access to IT systems, where the end users are actually have no knowledge about the existence of such policies or procedures.

Information security are totally depends on the humans' involvement in the process of securing the information from any threats. Each employee must have the right attitude towards protecting the information in the organization. Information security awareness program should also contribute to in teaching the organizational employees on the awareness but however current programs fail to pay necessary attention to employee behavioral theories.

Secondly, the development of an organizational culture of information security is necessary in order to ensure that the organization's employees have the minimal knowledge towards information security and the impact to the organization. Research shows that information security has shown that the combination of technical and non-technical approaches is needed in order to secure information systems for an organization.

System administrator should emphasis more on the technical approach such as manage and standardized the installed applications, monitor the traffic in and out of the organization or encrypted the local drives in the systems to avoid the end users from abusing the available data. Meanwhile the non-technical approach should also get the major attention from the management level where user awareness which can be classified as the main goal to ensure all users are informed and aware of security risks that may take place in their daily activity at work environment.

1.3 Objectives

The primary objective of this research is to discuss on the perception with the system administrators' and end users' on their perceptions in enterprise security awareness. The objective of information security management to:

i. To classify the knowledge level of users' awareness in relation to security threats and risks.

ii. To determine the highest reported threats impacting the organization information's.

iii. To identify the perspective between the system administrator and end users' regarding the information security practices.

iv. To evaluate the formal and regular security awareness refresher programs conducted.

1.4 Research Questions

The research will focus on addressing the following questions:

i. What are the knowledge level of users' awareness in relation to security threats and risks?
ii. What is the highest reported security attacks that being addressed in the organization?
iii. What are the perspective between the system administrator and end users' regarding the information security practices in the organization?
iv. How many security awareness programs have been conducted in the organization?

1.5 Significance of the Research

The results of the research will be used to assist the information security team in developing a better approaches to implement awareness among the employee in the organization. It will help those non-technical methodologies where those change has been finalized in conjunction with the business needs.

Those outcomes of contemplate are likely with the help of the security steering's who are relying mainly on the technology devices for example, firewalls, server-based infection and etc. These will help them to investigate those information security impacts and factors in the organization. This research will help the system administrator to acknowledge their commitment in taking responsibility for data protection in the organization.

1.6 Scope

i. Data security begins to turn into an imperative benefits to the business environment. Huge numbers of analysis on data security administration was addressed mostly on technical and non-technical by utilizing the interview with the security operations, questionnaires and archival records. This research will be likewise directed among the employees who represented from the targeted team. The main target groups for this research are:

ii. Information Security Officer (ISO)

iii. Information Technology System Administrators

iv. Team Leads from Information Technology Operations, Infrastructure, Network, Active Directory

v. Executive from Project Management Office

vi. End users' from various departments.

1.7 Summary

This section displays the vitality about data security where the end users' contribution have been recognized as a standout among the weakest connection for the information security awareness. Both human information and co-operations in ensuring the data protection would truly require to support the end goal on the information security safeness. The administrator should instruct the end users to make sure all of them are well prepared on beat the information security dangers.

REFERENCES

Abdul Serwadda & Vir V.Phoba (2013), When kids' toys breach mobile phone security, CCS '13 Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 599-610

Adams, A., & Sasse, M. A. (1999). Users are not the enemy: why users compromise security mechanisms and how to take remedial measures. Communications of the ACM, 42 (12), 40-46.

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

Albrechtsen, E. (2007). Understand Security Behaviours in Practice, Computers &Security, Security Policy Institute, 139 - 265

Anderson, R. (2001). Security engineering: A guide to building dependable distributed systems. Wiley John Wiley & Sons.

Anderson, R., & Moore, T. (2007). Information Security Economics-and Beyond. Advances in Cryptology -CRYPTO7, 68-91.

Andrew Darnton, GSR Behaviour Change Knowledge Review, An overview of behaviour change models and their uses, Centre for Sustainable Development, July 2008

Anthony Vance (2010), Why Do Employees Violate is Security Policies? Department of Information Processing Science, University of Oulu, 10-15

Babbie, E. (2001). The practice of social research (9th ed). Belmont, CA Wadsworth Thomson Learning.

Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social engineering: assessing vulnerabilities in practice . European Information Security Multi-Conference, 17(1), 53-63.

Bel G. Raggad (2010), Information Security Management: Concepts and Practice, CRC Press

Benjamin Khoo, Peter Harris, Stephen Hartman (2010), International Journal of Management & Information Systems – Third Quarter 2010 Volume 14, Number 3, Information Security Governance Of Enterprise Information Systems: An Approach To Legislative Compliant, M. Whitman and H. Mattord, 2004

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

Brown, A.S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. Applied Cognitive Psychology, 18(6), 641-651.

Burd, S., Haschak, M., & Cherkin, S. (2007). 2nd Annual Symposium on Information Assurance. Retrieved November 20, 2008, from http://www.nysfirm.org/documents/pdf/csc-2006/iasymposium.pdf#page=18

Bruce Schneier (2008), Security Pitfalls In Cryptography, Counterpane System, 145-167

Carstens, D., McCauley-Bell, P., Malone, L. C., & De-Mara, R. (2004). Evaluation of the human impact of password authentication practices on information security. Informing Science Journal, 7, 67-86.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. Communications of the ACM, 47(7), 87-92.

Chen, C. C, Shaw, R. S., & Yang, S. C (2006). Mitigating information security risks by increasing user security awareness: a case study of an information security awareness system. Information Technology, Learning, and Performance Journal, 24(1), 1-14.

Creswell, J. W. (1998). Qualitative inquiry and research design: choosing among five traditions. Thousand Oaks, Calif: Sage Publications.

Creswell, J. W. (2003). Research design: qualitative, quantitative, and mixed method approaches. Thousand Oaks, Calif: Sage Publications.

Cormac Herley, Where Do Security Policies Come From?, Microsoft Research, 2010

Daniel Mellado, David G.Rosado (2008), An Overview of the Current Information, Volume 18, Issue 12, J.UCS Special Issue, 2012, Retrieved from Blanco, 2010 and Opdahl and Sindre, 2008

D'Arcy, J.,Hovav, A., & Galletta, D. (2008)User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research,Articles in Advance, 79-89

de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D., Ren, J., Rode, J., & Filho, R. S. (2005). Two experiences designing for effective security. In Proceedings of the 2005 Symposium on Usable Privacy and Security, USA, 93,25-34. Retrieved April, 2008, from http://doi.acm.org/10.1145/1073001.1073004

Dhillon, G. (2007).Principles of information systems security: text and cases. John Wiley & Sons, Hoboken, NJ.

Dinev, T., & Hu. Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. Journal of the Association for Information Systems, 8(7), 386-408.

Dodge Jr., R. C., Carver, C. & Ferguson, A. J. (2007). Phishing for user security awareness. Computers & Security, 26, (1), 73-80.

Egan, M. (2004). The executive guide to information security: threats, challenges, and solutions. Harlow: Addison-Wesley.

Ernst & Young Global Information Security Survey (2004), Annual Global Information Security Survey Report. Retrieved 25 September, 2008 from http://craigchamberlain.com/library/surveys/2008_Global_Information_Security_Survey2008.pdf.

Foltz, C. B., Cronan, T. P., & Jones, T. W. (2005). Have you met your organization's computer usage policy? Industrial Management and Data Systems, 105(2), 137-146.

Foltz C. B, Schwager, P. H., & Anderson J. E. (2008).Why users (fail to) read computer usage policies. Industrial Management + Data Systems, 108(6), 701-713.

Furnell, S. M. (2003). Vulnerability exploitation: the problem of protecting our weakest links. Computer Fraud & Security, 11, 12-15.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006).The challenges of understanding and using security: A survey of end-users. Computers & Security, 25(1), 27-35.

Gable, G. (1994). Integrating Case Study and Survey Research Methods: An Example in Information Systems. European Journal of Information Systems, 3(2), 112-126.

Garg, A., Curtis, J., & Halper, H. (2003). The Financial Impact of IT Security Breaches: What Do Investors Think? Information Security Journal: A Global Perspective, 12(1), 22 -33.

Gross, J. B. & Rosson, M. B. (2007). Looking for trouble: understanding end-user security management. In Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology (Cambridge, Massachusetts, March 30 - 31, 2007).

Hasan, R. & Yurcik, W. (2006). Beyond Media Hype: Empirical Analysis of Disclosed Privacy Breaches 2005-2006 and a DataSet/Database Foundation for Future Work", in The Workshop on the Economics of Securing the Information Infrastructure.

Herath, T. & Rao, H.R. (2009).Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems (2009) 18, 106–125.

Huang, D., Rau, P.P., & Salvendy, G. (2008). Perception of information security. Behaviour & Information Technology, 1-12.

Information Technology - Security techniques - Code of Practice for Information Security Management, Retrieved on December, 2008, ISO/IEC 27001:2005.

Jamison W. Scheeres, 2008, Establishing The Human Firewall: Reducing An Individual’s Vulnerability To Social Engineering Attacks, retrieved from Winkler, I.S & Deadly, B, 1995, 86-90

Janna-LynnWeber, 2010, Privacy and Security Attitudes, Beliefs and Behaviours: Informing Future Tool Design, Retrieved from Adams and Sasse’s, 1999, 51-89

Joshua B. Gross, Mary Beth Rosson (2007), Looking for trouble: understanding end-user security management, Symposium on Computer Human Interaction for Management of Information Technology, Cambridge, Massachusetts, USA

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

Kemi-Tornio, Ibrahim, Abduletife Abdulwhab (2012), A Case of Orange Gate Private Limited Company (OGPLC), Formulating Secure Information Communication Guidelines, University of Applied Science, 2012 Retrieved from Michael E. Whitman and Herbert J. Mattord, 2008

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289-296.

Kruger, H. A., & Kearney, W. D. (2008). Consensus ranking - An ICT security awareness case study. Computers & Security, 27(7-8), 254-259.

Kvavik, Robert B, John Voloudakis (2006), Safeguarding the Tower: IT Security in Higher Education 2006. ECAR, Volume 6, 2006, 136 pages

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. Behaviour & Information Technology, 27 (5), 445-454.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. Information Management & Network Security, 10(2), 57-63.

Leonard, L. N. K., Cronan, T. P., & Kreie, J.(2004). What influences IT ethical behavior intentions-planned behavior, reasoned action, perceived importance, or individual characteristics? Information and Management, 42(1), 143–159.

Leonard, L. N. K., & Cronan, T. P. (2005). Attitude toward ethical behavior in computer use: a shifting model. Industrial Management & Data Systems, 105(9), 1150-1171.

Lee, Larose, and Rifon, How do patients respond to violation of their information privacy?, Health Information Management Journal, 2008

MacNealy, M. S. (1997). Toward better case study research. Professional Communication, IEEE Transactions , 40(3), 182-196.

Markotten, D. G. (2002). User-Centered Security Engineering. Retrieved November 2007, from http://tserv.iig.uni-reiburg.de/telematik/atus/publications/Ge2002.pdf.

Mari Karjalainen (2011), Improving Employees' Information Systems (IS) Security Behavior, 2011

Maritza Johnson (2010), Optimizing a Policy Authoring Framework for Security and Privacy Policies, IBM T.J. Watson Research Center, 12-26

Maxion, R. A., & Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. International Journal of Human Computer Studies, 63 (1-2), 25-50.

M. R. Pattinson and C. Jerram, (2010), Examining End-user Perceptions of Information Risks**,** South African Information Security Multi-Conference, retrieved from Huang et al.

Michael Workman (2008), A test of interventions for security threats from social engineering, Security Policy Institute, 15

Michael E.Whitman and Herbert J. Mattord (2007), Principles of Information Security, Thomson Learning- Course Technology, 2nd Edition, 188 - 120

Ng,B., Kankanhalli, A., & Xu, Y. (2009). Studying user's computer security behavior: A health belief perspective. Decision Support Systems, 46, 815-825.

NIST Special Publication 800-39 (2011), Managing Information Security Risk, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. Proceedings of the40th Annual Hawaii International Conference on System Sciences (HICSS'07), 156b, IEEE Computer Society.

Patrick, A. S., Long, A. C., & Flinn, S. (2003). HCI and security systems. In CHI '03 Extended Abstracts on Human Factors in Computing Systems (Ft. Lauderdale, Florida, USA, April 05 - 10, 2003). CHI '03. ACM Press, New York, NY, 1056-1057. Retrieved April 10, 2007, from http://doi.acm.org/10.1145/765891.766146

Pirani, J.A., & Spicer, D. Z. (2006) .Most Improved: How Four Institutions Developed Successful IT Security Programs. EDUCAUSE Center for Applied Research, Research Study, Volume 5. Retrieved October 10, 2008, from http://connect.educause.edu/Library/ECAR/MostImprovedHowFourInstit/37704

Rhee, H.-S., Kim, C., and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 1-11.

Raees Khan (2010), Practical Approaches to Organizational Information Security Management, SANS Institute,. Retrieved from CoBIT 2005.

Rain Ottis (2010), Information Warfare & Security, Cybernetic, Cyber Defence Department, Tallinn Estonia

Ryan, J. E. (2006). A comparison of information security trends between formal and informal environments. Ph.D. dissertation, Auburn University, United States -- Alabama. Retrieved November 8, 2008, from Dissertations & Theses: Full Text database. (Publication No. AAT 3225287).

Rezgui and Marks (2008), Analysis of Characteristics of Victims in Information Security Incidents, Sixth International Symposium on Human Aspects of Information Security & Assurance

Robert Richardson (2008), Computer Crime & Security Survey, CSI Director, Computer Security Institute

Ross Anderson and Tyler Moore (2011), Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research, Computer Science Group, Harvard University, Cambridge, Massachusetts, 110-148

Salahuddin M. Alfawaz (2011), Information Security Mangement: A case study of an information security culture, Queensland University of Technology

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.

Schneier, B. (2000). Secrets & lies, Digital security in a networked world, John Wiley, New York .

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. SIGMIS Database, 38, (1), 60-80.

Siponen, M., Pahnila, S., and Mahmood, A., 2007, in IFIP International Federation for Information Processing, 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), 133-144.

Smetters, D. K., & Grinter, R. E. (2002). Moving from the design of usable security technologies to the design of useful secure applications. In Proceedings of the 2002 Workshop on New Security Paradigms (Virginia Beach, Virginia, September 23 - 26, 2002). NSPW '02. ACM, New York, NY, 82-89.

Steven Woodhouse (2007), Information security end user behavior and corporate culture, Department of Lands, 769

Stake, R. E. (1995). The art of case study research. Thousand Oaks: Sage Publications.

Stanton, J. S., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers and Security, 24(2), 124-133.

Straub, D. (1990). Effective IS security: an empirical study. Information Systems Research, 1(3), 255-276.

Suo, X., Zhu, Y., & Owen, G. S. (2005). Graphical Passwords: A Survey. In Proceedings of the 21st Annual Computer Security Applications Conference (December 05 - 09, 2005). ACSAC. IEEE Computer Society, Washington, DC, 463-472.

Tamara, D. & Qing, H. (2007).The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. Journal of the Association for Information Systems, 8(7), 23, 386-408.

Tejaswini Herath, H.R. Rao, (2009), Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, Decision Support Systems, Science Direct, Volume 47, Issue 2, retrieved from Dhillon, 2007

Thomas, T. M. (2004). Network security first-step. First-step series. Indianapolis, IN: Cisco Press.

Thomson, M., & von Solms, R. (1998). Information Security Awareness: educating your users effectively. Information Management and Computer Security ,6(4), 167-173.

Trcek, D., Trobec, R., Pavesic, N., & Tasic, J. F. (2007). Information systems security and human behaviour. Behaviour and Information Technology, 26(2), 113-118.

Vicente, K. J. (2004). The human factor: Revolutionizing the way people live with technology. New York: Routledge.

Victoria Mahabi (2010), Information Security Awareness: System Administrators and End-users Perspectives at Florida, State University, Retrieved from Hasan & Yurcik, 2008-2010.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. Computers and Security, 23(3), 191-198.

Wagner, A. E., & Brooke, C. (2007). International Access Management: Making Access Control Usable For End Users. Journal of Business Research Methods, 5(2), 117-124.

Weir,C. S., Douglas,G., Carruthers,M. & Jack,M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. Computers & Security, 28(1-2), 47-62.

Weirich, D. & Sasse, M. A. (2001). Pretty good persuasion: a first step towards effective password security in the real world. In Proceedings of the 2001 Workshop on New Security Paradigms (Cloudcroft, New Mexico, September 10 - 13, 2001). NSPW '01. ACM, New York, NY, 137-143.

Wiant, T. L. (2005). Information security policy's impact on reporting security incidents, Computers & Security, 24(6), 448-459.

Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. (2006). Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the Working Conference on Advanced Visual interfaces (Venezia, Italy, May 23 - 26, 2006). AVI '06. ACM, New York, NY, 177-184.

Winkler, I. S., & Dealy, B. (1995). Information Security Technology? Don"t Rely on It. A Case Study in Social Engineering. The Fifth USENIX Unix Security Symp.,Salt Lake City, Utah, 1-6, June 5-7.

Wixom, B. H., & Todd, P. A. (2005). A theoretical integration of user satisfaction and technology acceptance. Information Systems Research, 16(1), 85-102.

Woodhouse, S. (2007). Information Security: End User Behavior and Corporate Culture. In Proceedings of the 7th IEEE international Conference on Computer and information Technology (October 16 - 19, 2007). CIT. IEEE Computer Society, Washington, DC, 767-774.

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A protection motivation theory approach to home wireless security. International Conference on Information Systems, Las Vegas,Vol. 26, 367–380.

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. Information Security Journal: A Global Perspective, 16(6), 315-331.

Workman, M. (2008). A test of interventions for security threats from social engineering. Information Management & Computer Security, 16(5), 463- 483.

Workman,M., Bommer,W.H., & Straub,D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799-2816.

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2005). Password memorability and security: empirical results. Security & Privacy, IEEE , 2(5), 25-31.

Yin, R. K. (1984). Case study research: design and methods. Applied social research methods series. Beverly Hills, Calif: Sage Publications.

Yin, R. K. (1993). Applications of case study research. Applied social research methods series, v. 34. Newbury Park, Calif: SAGE Publications

Yin, R. K. (1994). Case study research: Design and methods. Applied social research methods series, v. 5. Thousand Oaks: Sage Publications.

Youn, S.(2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. The Journal of Consumer Affairs, 43(3), 389 - 418.

Zurko, M. E., Kaufman, C., Spanbauer, K., & Bassett, C. (2002). Did you ever have to make up your mind? What notes users do when faced with a security decision. Proceedings of 18th Annual Computer Security Applications Conference. Las Vegas, Nevada, 371-381.

Zurko, M. E. (2005).User-Centered Security: Stepping Up to the Grand Challenge. acsac. 187- 202. Retrieved November 20, 2008, from http://doi.ieeecomputersociety.org/10.1109/CSAC.2005.60