DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's full name : MEHRDAD MANSOURI

Date of birth : 19/09/1985

Title : EVALUATING INFORMATION SECURITY CULTURE IN HIGHER LEARNING INSTITUTION

Academic Session : 2, 2011/2012

I declare that this thesis is classified as :

☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)*

■ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:

1. The thesis is the property of Universiti Teknologi Malaysia.
2. The Library of Universiti Teknologi Malaysia has the right to make copies for the Purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by :

SIGNATURE	**SIGNATURE OF SUPERVISOR**
N15732142	**Assoc. Prof. Dr. Zuraini Ismail**
(NEW IC NO. /PASSPORT NO.)	**NAME OF SUPERVISOR**
Date :	Date :

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of the degree of Master of Information security.

Signature : .....

Name of Supervisor : Assoc. Prof. Dr. Zuraini Ismail

Date : 20/06/2012

EVALUATING INFORMATION SECURITY CULTURE IN HIGHER LEARNING INSTITUTION

Mehrdad Mansouri

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

Center for Advanced Informatics School (AIS)
Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JUNE 2012

I declare that this thesis entitled “Evaluating Information Security Culture in Higher Learning Institution” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : .....

Name : Mehrdad Mansouri

Date : 20/06/2012

ACKNOWLEDGEMENTS

I would have never been able to finish this project paper without the encouragement of Advanced Informatics School (AIS), my family, and friends whose assistance, support, and cooperation sustained me throughout the entire time.

First and foremost, I would like to express my sincere appreciation to my supervisor, Assoc. Prof. Dr. Zuraini Ismail. I have been very lucky to have this opportunity to learn from her. I was overwhelmed by her knowledge, insightful advice, professionalism, and guidance during this thesis. She provided me with a role model of a professor and researcher that I wish to emulate in my future career. I also thank her for believing in my abilities with insightful patience. I am honoured that I will graduate as her master student, and I hope that we can continue working together as collaborators, as well as be good friends.

Then, I would like to appreciate my beloved parents who supported me and patiently accompanied with me during this survey.

ABSTRACT

Information security culture plays the crucial role in Higher Learning Institutions, thus cultivating information security culture is a major challenge in many universities. This study aims to evaluate the impact of information security culture among public universities in Klang Valley, Malaysia and proposes the model for cultivating information security culture through three major components which are Corporate Governance, Management Support, and Employee Security Management. This particular study applied quantitative research methodology and the questionnaires have been distributed among academic and administrative staff of IT faculties in public universities in Malaysia. Three hypotheses were tested and the findings showed that they were accepted to reach three main objectives, but the relationship between corporate governance and cultivating information security culture is more stronger than the other components. The results revealed that the management should demonstrate some information security privacy and policies and encourage the staff to adhere to them. The management should also train the employees through some awareness programs to avoid any kind of threats in the future. Finally, providing information security risk assessments help Higher Learning Institutions to identify threats and minimize risks.

ABSTRAK

Pembudayaan keselamatan maklumat memainkan peranan yang amat penting didalam Institusi Pengajian Tinggi, seterusnya memupuk pembudayaan keselamatan maklumat adalah cabaran yang utama di kebanyakkan universiti. Objektif kajian ini adalah untuk menilai kesan ke atas pembudayaan keselamatan maklumat dikalangan universiti awam di lembah Klang, Malaysia dan mencadangkan model untuk memupuk pembudayaan keselamatan maklumat melalui tiga komponen iaitu Pentadbiran Korporat, Sokongan Pengurusan dan Pengurusan Keselamatan Pekerja. Kajian ini mengaplikasikan metod kajian quantitatif dan soalan kajian yang telah diberikan di kalangan kakitangan akademik dan kakitangan pentadbiran di dalam jabatan atau fakulti IT di dalam universiti awam. Tiga hipotesis yang telah diuji dan keputusan kajian memberi keputusan yang signifikan dan diterima. Keputusan kajian membuktikan bahawa sokongan pengurusan perlu menunjukkan beberapa privasi maklumat keselamatan dan dasar-dasar dan menggalakkan kakitangan untuk mematuhi kepada mereka. Pihak pengurusan juga perlu melatih pekerja melalui beberapa program kesedaran untuk mengelakkan sebarang ancaman di masa depan. Akhirnya, menyediakan penilaian risiko keselamatan maklumat membantu Institusi Pengajian Tinggi untuk mengenal pasti ancaman dan meminimumkan risiko.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IS	-	Information Systems
IT	-	Information Technology
ICT	-	Information and Communication Technology
HLIs	-	Higher Learning Institution
CSI	-	Computer Security Institute
ISRAs	-	Information Security Risk Assessments
UPM	-	University Putra Malaysia
UKM	-	University Kebangsaan Malaysia
UTM	-	University Technology Malaysia
UM	-	University Malaya
CG	-	Corporate Governance Items
MS	-	Management Support Items
ESM	-	Employee Security Management Items
ISC	-	Cultivation Information Security

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

It is obvious that Information and Communication Technology (ICT) progress influence all parts of society which Higher learning Institution (HLIs) are not detached from them. Colleges and universities have lots of networks and computer systems. The more usage of computer systems (Al-Salihy *et al.*, 2003) causes institutions develop their learning methods automatically based on the major recent alterations (Bakari *et al.*, 2005). Nowadays, preparing a high secure level for networks and computer is one of the main issues for institutions (Luker *et al.*, 2003).

Information has a crucial role in today's world. Institutions are one part of the world that cannot operate without computers (Pfleeger and Pfleeger, 2007). This high usage of information and computers results in vulnerability of institutions. Thus, they should protect their computers and networks from all kinds of threats and risks. Hence, institutions all around the world including Malaysia should adopt different types of monitoring for their systems to protect their information (Millar *et al.*, 2005).

At the present time, the realization of information security as a business issues not an IT one and the difference between them is one of the major points of researchers' challenging items. Development of information as a strategic property and computerizing of information systems are two tactical instruments for organizations and governments (Calder, 2006; McCumber, 2005; Moskowitz and

Kern, 2003; Sherwood *et al.*, 2005). For safety of information, some information security tools and strategies are adopted which give considerable value to any organization specially HLIs (Hagen *et al.*, 2008).

According to Peltier (2005), the most important risk to information of an organization and its computer systems is due to its employees because the most of organizational computer attacks occur internally (AusCERT, 2005). Organization's employees have all the details of procedures and awareness of where information properties are kept and how they are protected. By estimation of the Computer Security Institute (CSI) in San Francisco, USA, between 60% - 80% of all network misgiving is caused by employees of organizations (Peltier *et al.*, 2005). The threat of employee to the information assets of the organization has been discussed by researchers especially over the previous decade. Internal threats were the major category of organizational attacks in the Office of Strategic Crime Assessments (OSAC, 1997) Computer Crime and Security Survey.

Overall, the impact of organizational culture is very high on the success or failure of the organization. The organizational culture determines employees' action when an organization encountered a problem or threat by analyzing, giving definitions, and solution to the problem (Robbins Stephen, 2005). Consequently, each organization should adopt some security affairs to its organizational culture to decrease risks and threats of information assets. This issue leads to automatically pay attention of all employees and managers to secure their designing, organizing and operational activities (Woodhouse, 2007).

1.2 Background of the Study

Lots of information security incidents such as hacking and website's attack have been occurred in recent years and various personal data were rifled. Thus, organizations are encountered considerable attacks and risks which may damage private data of an organization (Directory, 2009). Information security has been displaced its situation from mainframe computers to the recent place of complicated Internet. New threats have been raised by new technological advancement and progress. Researchers demonstrate that information security targets have been spread out and its concentration has been changed to strategic governance. Thus, internal and international society should more concentrate on information security issues (Dlamini *et al.*, 2009).

Information security is a sophisticated technological procedure. The increasing complicacy and progress of threats demonstrate the necessity of adopting security programs in organizations (Kumar, 2009). Increasing usage of information and sharing computer data through the Internet enhanced the organizational attacks. The socio-cultural methods can increase the current technical and organizational process to enhance employee information security awareness which results in elevating the entire organizational security level (Schlienger and Teufel, 2003).

In recent years, information security researches show that organizations use information security culture which includes "people, processes, technology, and operations capabilities" of the organizations to avert threats to their information asset (Allen, 2005; FFIEC, 2006; NIST, 2008). Furthermore, "technology-driven security solutions" are not sufficient to defend an organization from information threats, because information technologies are progressing and advancing rapidly (Alberts *et al.*, 2001; Alberts and Hayes, 2003; Caralli, 2004).

Information and information security have been became significant issues in Higher learning Institution (HLIs) in the last decades. Development of information

technology has increased the level of information risks and threats without any achievement and progress and advancement in the management and cultivation of information security culture in the developing countries (Bakari *et al.*, 2005). Their roles are to improve total HLIs aims which lead to specific competitive advantages (SaugatuckTechnology, 2008; Schultz, 2006; Tallon *et al.*, 2000; Wood, 1993).

Nowadays, most of organizations consider information as a crucial organizational property that helps the organization to be successful globally in the society (FFIEC, 2006; Kaplan and Norton, 2007; McFadzean *et al.*, 2007; Senge, 1990; Straub, 1990). Therefore, information security has moved beyond the boundaries and became a challenging issue to prevent complicated information security threats (Alberts and Hayes, 2003; Anderson and Choobineh, 2008; Park and Ruighaver, 2008; Symantec, 2009).

1.3 Problem Statement

Researchers considered information as an organizational property for all kinds of organizations including HLIs. Thus, one of the major issues which cause main challenges to the organizations all around the word is information security (PricewaterhouseCoopers, 2008; TechAmerica, 2009; Young, 2007, 2008). Organizations make information security as a strategic tool to prevent the attacks to their information and securely protect it (Amaio, 2009; Ezingeard *et al.*, 2005; Wood, 1993). Therefore, operative information security culture will aid the organization to securely protect its information property in such a sophisticated environment.

Therefore the first issue which cause this study began was the importance of Information Systems (IS) security and confidentiality in HLIs. Information security is not a recent issue; it was considered from the 1970s (Kerievsky, 1976), but a few studies have been done in this case (Steffani, 2006). However, the influence of

organizational information security culture on employee's attitude is discussed by Dontamsetti and Narayananb (2009). Based on their studies, the effectiveness of organization's information security culture and the process of keeping information securely are not sufficient.

Secondly, based on the survey of MyCERT, CyberSecurity Malaysia (Mycert, 2008), 10,354 security misadventure including spam incidents totally happened in the first quarter 2008. Compared to fourth quarter in 2007, there is a 5.59% growth of incidents which were included "intrusion, hack threat, malicious code, denial of service and spam". If Malaysian organizations do not adopt proper protections for their systems, it is impossible to avoid computer crimes on those organizations. "Computer viruses, natural disaster and negligence" are the major computer crimes which have been considered. Finally, the most important reason of these crimes has been revealed as lack of awareness about information, software and hardware threats and risks among employees (Kundu, 2004).

Thirdly, it has been considered that HLIs have not suitable information security awareness and training programs (North *et al.*, 2006). Additionally, most of these training programs and researches have been implemented in developed countries. Thus, the researches in developing countries such as Malaysia are not sufficient (Marks and Rezgui, 2009).

Finally, due to storing and processing lots of information electronically, the loss of information security has been increased. The misgiving of these data happens because information technology is naturally vulnerable (Chiu and Chen, 2005). A series of network security threat have been appeared to HLIs in Malaysia which originate from the growth of complex procedure of attack and a mix of specific kind of risk (Garuba *et al.*, 2008). The investigation of attacks and security misadventure which are recorded by "Malaysia Computer Emergency Response Team (MyCERT, 2009), a department within CyberSecurity Malaysian 2009", shows that only 34% of misadventure handled respectively (Ismail *et al.*, 2010). As Higher Learning Institutions have large amount of data and computers and also their employees and

the public can freely access to their information, they are so vulnerable to cyber-attacks (Katz, 2005).

Hence, these gaps have been considered in Malaysian HLIs which reveal that each Higher Learning Institute needs to apply the proper information security culture as an essential part of their institutions to mitigate or even prevent these kinds of attacks and threats.

1.4 Research Questions

These research questions have been considered as a direction and guidance to gain the research's objectives.

i. What are the components of information security culture in Higher Learning Institution?

ii. How to design information security culture model for the Higher Learning Institution?

iii. How to cultivate an information security culture in Higher Learning Institution based on the proposed model?

1.5 Project Aim

As long as the potency of university to prevent and manage threats of its information property has been considered as an important issue of information security (Baker and Wallace, 2007), this study is aimed to determine the impact of "information security culture" among academic and administrative staff of IT and computer science faculties of four public research universities in Klang Valley.

The study examines different characteristics of organizational culture such as corporate governance, management support, and employee security management which result in cultivating information security culture in Higher Learning Institutions. The result of this research can be applied as a recommendation for the progress of "Information Security Culture" model and can be proposed to Malaysian HLIs to improve their information security procedures.

1.6 Research Objectives

This research has three main objectives which are:

i. To identify the components of information security culture.

ii. To propose and design the information security culture model in Higher Learning Institutions.

iii. To evaluate the proposed information security culture model in Higher Learning Institutions.

1.7 Research Scope

The scope of this study was focused on four Higher learning Institutions located in Klang Valley, Malaysia. The research study was conducted by distributing questionnaires among academic and administrative staff of IT and computer science faculties of these four public research universities which are University Malaya (UM), University Putra Malaysia (UPM), University Kebangsaan Malaysia (UKM), and University Technology Malaysia (UTM).

1.8 Significance of the Study

This research has concentrated on information security culture within the public research universities located in Klang Valley, Malaysia. It will help academic and administrative staff of IT and computer science faculties to improve their existing information security culture and will also act as a guide for implementing information security culture within the university. The study will provide suitable recommendations for the universities to cultivate their information security culture (Hayden, 2010). From the academic perspective, this particular research study extends the entire body of knowledge in information security culture in three phases which will mention in the next chapter.

1.9 Summary

This chapter begins with an overview of the importance of information security culture and its implication to various sectors including education sector, and followed by the background of the study. A series of network security threats, lack of proper information security awareness programs, and finally lack of effective studies related to higher learning institutions in Malaysia have led to the problem statement and subsequently defining the research questions. The project's aims were then discussed followed by research objective. Afterwards, research scope, significance of the study, and the summary of this chapter explained respectively. The next chapter presents the review of the Information Security culture literature.

REFERENCES

Al-Salihy, W., Ann, J., and Sures, R. (2003). Effectiveness of information systems security in IT organizations in Malaysia 716-720 Vol. 712.

Alberts, D. S., Garstka, J. J., Hayes, R. E., and Signori, D. A. (2001). *Understanding information age warfare*: DTIC Documento. Document Number)

Alberts, D. S., and Hayes, R. E. (2003). *Power to the edge: Command... control... in the information age*: DTIC Documento. Document Number)

Allen, J. (2005). *Governing for enterprise security*: DTIC Documento. Document Number)

Amaio, T. E. (2009). *Exploring and examining the business value of information security: Corporate executives' perceptions*. ProQuest.

Anderson, E. E., and Choobineh, J. (2008). Enterprise information security strategies. *Computers & Security.* 27(1), 22-29.

AusCERT. (2005). Australian Computer Crime & Security Survey. from http://www.auscert.org.au/

Baars, R. M., Atherton, C. I., Koopman, H. M., Bullinger, M., and Power, M. (2005). The European DISABKIDS project: development of seven condition-specific modules to measure health related quality of life in children and adolescents. *Health Qual Life Outcomes.* 3, 70.

Bakari, J. K., Tarimo, C. N., Yngstrom, L., and Magnusson, C. (2005). State of ICT security management in the institutions of higher learning in developing countries: Tanzania case study 1007-1011.

Baker, W. H., and Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. *Security & Privacy, IEEE.* 5(1), 36-44.

Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems.* 1(2), 121-130.

Beach, L. R., and Burns, L. R. (1995). The service quality improvement strategy: identifying priorities for change. *International Journal of Service Industry Management.* 6(5), 5-15.

Bennett, C., and Regan, P. M. (2004). Editorial: surveillance and mobilities. *Surveillance & society.* 1(4), 449-455.

Caelli, W. J., Longley, D., and Shain, M. (1989). *Information security for managers*. Groves Dictionaries, Inc.

Calder, A. (2006). *A business guide to information security: how to protect your company's IT assets, reduce risks and understand the law*. Kogan Page Ltd.

Caralli, R. A. (2004). for Enterprise Security, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA. from www.sei.cmu.edu/reports/04tn046.pdf

Chen, C. C., Medlin, B. D., and Shaw, R. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security.* 16(4), 360-376.

Chia, P., Maynard, S., and Ruighaver, A. (2002). Understanding organizational security culture. *Proceedings of PACIS2002. Japan*.

Chiu, R. K., and Chen, J. C. H. (2005). A generic service model for secure data interchange. *Industrial Management & Data Systems.* 105(5), 662-681.

CISSP, S. H. (2001). Designing a security awareness program: Part 1. *Information Systems Security.* 9(6), 1-9.

Da Veiga, A., and Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computers & Security.* 29(2), 196-207.

de Freitas Corresponding, S., and Oliver, M. (2005). Does E-learning Policy Drive Change in Higher Education?: A case study relating models of organisational change to e-learning implementation. *Journal of Higher Education Policy and Management.* 27(1), 81-96.

den Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., and Vraalsen, F. (2007). Model-based security analysis in seven steps—a guided tour to the CORAS method. *BT Technology Journal.* 25(1), 101-117.

DesPlanques, D. (2005). *D.'Information Security Policy Development for Institutions of Higher Education,".* Thesis for Master. Regis University, School for

Professional Studies. 2005. Retrieved on October 14, 2008, from: http://www.academic. regis. edu/cias/ia/DesplanquesProfessionalProject. doc.

Detert, J. R., Schroeder, R. G., and Mauriel, J. J. (2000). A framework for linking culture and improvement initiatives in organizations. *Academy of management Review*, 850-863.

Directory, T. I. (2009). An Introduction of ISO 27001. *ISO27001 Section*.

Dlamini, M., Eloff, J. H. P., and Eloff, M. (2009). Information security: The moving target. *Computers & Security.* 28(3-4), 189-198.

Dontamsetti, M., and Narayanan, A. (2009). Impact of the human element on information security. *Social and Human Elements of Information Security: Emerging Trends*.

Ezingeard, J. N., McFadzean, E., and Birchall, D. (2005). A model of information assurance benefits. *EDPACS.* 32(11), 1-16.

FFIEC.(2006). Information Security Booklet. from www.ffiec.gov/ffiecinfobase/ book lets/information_security/information_security.pdf

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

Garuba, M., Liu, C., and Washington, N. (2008). A comparative analysis of anti-malware software, patch management, and host-based firewalls in preventing malware infections on client computers 628-632.

Gerber, M., and von Solms, R. (2005). Management of risk in the information age. *Computers & Security.* 24(1), 16-30.

Gerber, M., von Solms, R., and Overbeek, P. (2001). Formalizing information security requirements. *Information Management & Computer Security.* 9(1), 32-37.

Hagen, J. M., Albrechtsen, E., and Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security.* 16(4), 377-397.

Hayden, L. (2010). IT security metrics: a practical framework for measuring security & protecting data. *Recherche.* 67, 02.

Herath, T., and Rao, H. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems.* 47(2), 154-165.

Hogganvik, I. (2007). A graphical approach to security risk analysis. *Oslo, Norway, Norway: University of Oslo-Faculty of Mathematics and Natural Sciences*.

Höne, K., and Eloff, J. (2002a). What makes an effective information security policy? *Network Security.* 2002(6), 14-16.

Höne, K., and Eloff, J. H. P. (2002b). Information security policy—what do international information security standards say? *Computers & Security.* 21(5), 402-409.

Hong, K. S., Chi, Y. P., Chao, L. R., and Tang, J. H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security.* 14(2), 104-115.

Ismail, Z., Masrom, M., Hamzah, D., and Sidek, Z. (2010). Information security considerations for higher learning institutions 1537-1542.

ISP. (2009). Information Security Policy World. The Security Policies & Standards Group, London. *Information Security Policy Objectives*, from http://www.information-security-policies-and-standards.com/objective.html.

Johnston, A. C., and Warkentin, M. (2008). Information privacy compliance in the healthcare industry. *Information Management & Computer Security.* 16(1), 5-19.

Kaplan, R. S., and Norton, D. P. (2007). 2.3 Using the balanced scorecard as a strategic management system. *Supplementary Readings*, 62.

Katz, F. H. (2005). The effect of a university information security survey on instruction methods in information security 43-48.

Kerievsky, B. (1976). Security and confidentiality in a university computer network. *ACM SIGUCCS Newsletter.* 6(3), 9-11.

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

Kumar, V. (2009). *Symantec Global Internet Security Threat Report*: Symanteco. Document Number)

Kundu, S. C. (2004). Impact of computer disasters on information management: a study. *Industrial Management & Data Systems.* 104(2), 136-143.

Luker, M. A., Petersen, R. J., and EDUCAUSE. (2003). *Computer and Network Security in Higher Education*. Jossey-Bass.

Mackey, A., and Gass, S. M. (2005). *Second language research: Methodology and design*. Lawrence Erlbaum.

Marks, A. (2007). *Exploring universities' information systems security awareness in a changing higher education environment.* Ph. D. Thesis, University of Salford.

Marks, A., and Rezgui, Y. (2009). A comparative study of information security awareness in higher education based on the concept of design theorizing 1-7.

McCumber, J. (2005). *Assessing and managing security risk in IT systems: A structured methodology*. CRC Press.

McFadzean, E., Ezingeard, J. N., and Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review.* 31(5), 622-660.

Millar, C. C. J. M., Eldomiaty, T. I., Choi, C. J., and Hilton, B. (2005). Corporate governance and institutional transparency in emerging markets. *Journal of Business Ethics.* 59(1), 163-174.

Mitropoulos, S., Patsos, D., and Douligeris, C. (2007). Incident response requirements for distributed security information management systems. *Information Management & Computer Security.* 15(3), 226-240.

Moskowitz, K., and Kern, H. (2003). Managing IT as an investment.

Mycert. (2008). MS-130.052008: MyCERT Quarterly Summary (Q1) 2008. from http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/579/index.html

MyCERT. (2009). CyberSecurity-E-Security: MS-151.021009: MyCERT Quarterly Summary (Q4)2009, Cyber Security Malaysia., from http://www.cybersecurity.my/data/content_files/16/582.pdf?.diff=121750.

Myers, M. D. (2008). *Qualitative research in business & management*. Sage Publications Ltd.

NIST. (2008). Draft NIST Special Publication 800-39, Information Security – Managing Risk from Information Systems: An Organizational Perspective. from http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf

North, M. M., George, R., and North, S. M. (2006). Computer security and ethics awareness in university environments: a challenge for management of information systems 434-439.

OSAC. (1997). *Computer Crime and Security Survey.Office of Strategic Crime Assesments and Victoria Police Computer Crime Investigation Squad* o. Document Number)

Ott, L., and Longnecker, M. (2008). *An introduction to statistical methods and data analysis*. Duxbury Pr.

Park, S., and Ruighaver, T. (2008). Strategic approach to information security in organizations 26-31.

Peltier, T. R. (2002). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Auerbach Pub.

Peltier, T. R., Peltier, J., and Blackley, J. A. (2005). *Information security fundamentals*. CRC Press.

Pfleeger, C. P., and Pfleeger, S. L. (2007). Security in Computer. *Prenice Hall*.

Pipkin, D. L. (2000). *Information security: protecting the global enterprise*. Prentice-Hall, Inc.

Post, G. V., and Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security.* 26(3), 229-237.

PricewaterhouseCoopers. (2008). PWC global state of information security survey 2008 improving security: an action plan. from www.pwc.com/gx/ en/ informationsecurity-survey/index.jhtml

Qayoumi, M. H., and Woody, C. (2005). Addressing Information Security Risk. *EDUCAUSE QUARTERLY.* 28(4), 7.

Rezgui, Y., and Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security.* 27(7-8), 241-253.

Robbins Stephen, P. (2005). *Essentials of organizational behavior*. Prentice Hall.

Roper, C. A. (1999). *Risk management for security professionals*. Butterworth-Heinemann.

Sasaki, H., Ikeda, Y., Kondo, M., and Nakamura, H. (2007). An intra-task dvfs technique based on statistical analysis of hardware events 123-130.

SaugatuckTechnology. (2008). Enterprise information management for competitive advantage. from www.synaptica.com/djcs/synaptica/ Enterprise%20 Inform ation%20MgmtDJWhitepaper033108.pdf

Schein, E. H. (2004). *Organizational culture and leadership*. (Vol. 1): Jossey-Bass Inc Pub.

Schlienger, T., and Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture 405-409.

Schultz, E. E. (2006). The changing winds of information security. *Computers & Security.* 25(5), 315-316.

Sekaran, U. (2006). *Research methods for business: A skill building approach*. Wiley-India.

Senge, P. M. (1990). *The fifth discipline: The art and practice of the learning organization*. Random House.

Shedden, P. A. (2006). A and Ruighaver, AB (2006) Risk Management Standards–The Perception Of Ease Of Use 19-20.

Sherwood, J., Clark, A., and Lynas, D. (2005). Enterprise security architecture. *COMPUTER SECURITY JOURNAL.* 21(4), 24.

Sons, J. W. a. (1999). *The Value Nef, A Tool for Competitive Strategy*. Parolini.

Steffani. (2006). The Impact of Information Security in Academic Institutions on Public Safety and Security: Assessing the Impact and Developing Solutions for Policy And Practice., from http://dx.doi.org/10.3886/ICPSR21188.

Straub, D. W. (1990). Effective IS security. *Information Systems Research.* 1(3), 255-276.

Symantec. (2009). Symantec internet security threat report trends for 2008. from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_ internet_security_threat_report_xiv_04-2009.en-us.pdf

Tallon, P. P., Kraemer, K. L., and Gurbaxani, V. (2000). Executives' perceptions of the business value of information technology: a process-oriented approach. *Journal of Management Information Systems*, 145-173.

TechAmerica. (2009). Nineteenth annual survey of federal chief information officers. from www.techamerica.org/techamerica-and-grant-thornton-release-19th-annual-survey-offederal-cios

Thomson, K. L., von Solms, R., and Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security.* 2006(10), 7-11.

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

Tudor, J. K. (2006). *Information security architecture: an integrated approach to security in the organization*. CRC Press.

Updegrove, D., and Gordon, W. (2003). Computers and Network Security in Higher Education.

Van Niekerk, J., and Von Solms, R. (2006). Understanding information security culture: A conceptual framework. *Information Security South Africa (ISSA), Johannesburg, South Africa*.

Varney, C. A. (1996). *Consumer privacy in the information age: a view from the United States*. US FTC.

Visintine, V. (2003). An introduction to information risk assessment. *SANS institute.8*

Von Solms, B. (2001). Corporate governance and information security. *Computers & Security.* 20(3), 215-218.

Von Solms, R., and von Solms, B. (2004). From policies to culture. *Computers & Security.* 23(4), 275-279.

Whitman, M. E., and Mattord, H. J. (2011). *Principles of information security*. Course Technology Ptr.

Wood, C. C. (1993). Achieving competitive advantage with information security. *Information Management & Computer Security.* 8(2), i-iv.

Woodhouse, S. (2007). Information security: end user behavior and corporate culture 767-774.

Young, E. a. (2007). Ernst & Young 2007's global information security survey. from www2.eycom.ch/publications/items/2007_giss/2007_ey_giss.pdf

Young, E. a. (2008). Ernst & Young 2008's global information security survey. from www.ey.com/Publication/vwLUAssets/GISS_2008/$FILE/GISS2008.pdf

Zakaria, O., and Gani, A. (2003). A conceptual checklist of information security culture.