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
(NEW IC NO./PASSPORT NO.)

Assoc. Prof. Dr. Zuraini Ismail

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

# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td></td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td></td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td></td>
<td>vi</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td></td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xi</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td></td>
<td>xii</td>
</tr>
<tr>
<td>LIST OF APPENDICES</td>
<td></td>
<td>xiii</td>
</tr>
</tbody>
</table>

1 INTRODUCTION

1.1 Overview 1
1.2 Background of the Study 3
1.3 Problem Statement 4
1.4 Research Questions 6
1.5 Project Aim 6
1.6 Research Objectives 7
1.7 Research Scope 6
1.8 Significance of the Study 8
1.9 Summary 8

2 LITERATURE REVIEW

2.1 Introduction 9
2.2 Information 9
2.3 Information Security 10
2.4 Information Security Culture 11
2.5 Corporate Governance 12
2.6 Management Support 14
2.7 Employee Information Security Management 17
2.8 Cultivating Information Security Culture 19
2.9 Proposed Model 20
2.10 Summary 23

3 RESEARCH METHODOLOGY
3.1 Introduction 24
3.2 Research Design 24
3.3 Operational Research Framework 27
  3.3.1 Planning Phase 27
    3.3.1.1 Problem Formulation 27
    3.3.1.2 Research Population and Sampling 28
  3.3.2 Analysis Phase 29
  3.3.3 Designing phases 29
    3.3.3.1 Questionnaire Design 29
  3.3.4 Implementation phases 31
  3.3.5 Testing phases 31
3.4 Summary 31

4 FINDING AND ANALYSIS
4.1 Introduction 32
4.2 Analysis of Demographic Profile 32
4.3 Analysis of Variables 36
  4.3.1 Analysis of Corporate Governance Variable 37
  4.3.2 Analysis of Management Support Variable 38
  4.3.3 Analysis of Employee Security Management Variable 40
  4.3.4 Analysis of Cultivation of Information Security Variable 42
4.4 Reliability Statistics 44
4.5 Regression Analysis 45
4.6 Summary 49

5 DISCUSSION AND CONCLUSION
5.1 Introduction 50
5.2 Summary of the Findings 50
5.3 Limitations and Recommendations of Future Research 52
5.4 Concluding Remark 53

REFERENCES 54
Appendices A-G 62-85
# LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Information Security Issues Which Illustrate</td>
<td>12</td>
</tr>
<tr>
<td>3.1</td>
<td>Deliverable Of Study Based on Research Objectives</td>
<td>26</td>
</tr>
<tr>
<td>3.2</td>
<td>Sampling Methodology</td>
<td>28</td>
</tr>
<tr>
<td>3.3</td>
<td>Structure of Questionnaire Design</td>
<td>30</td>
</tr>
<tr>
<td>4.1</td>
<td>Demographic Profile</td>
<td>34</td>
</tr>
<tr>
<td>4.2</td>
<td>Corporate Governance Items and their Related Codes</td>
<td>37</td>
</tr>
<tr>
<td>4.3</td>
<td>Management Support Items and their Related Codes</td>
<td>39</td>
</tr>
<tr>
<td>4.4</td>
<td>Employee Security Management Items and their Related Code</td>
<td>41</td>
</tr>
<tr>
<td>4.5</td>
<td>Cultivation of Information Security Items and their Related Codes</td>
<td>43</td>
</tr>
<tr>
<td>4.6</td>
<td>Cronbach Alpha</td>
<td>45</td>
</tr>
<tr>
<td>4.7</td>
<td>Regression Analysis</td>
<td>46</td>
</tr>
<tr>
<td>4.8</td>
<td>Regressions Analysis Model</td>
<td>47</td>
</tr>
<tr>
<td>4.9</td>
<td>Pearson’s Correlations for Each Construct</td>
<td>47</td>
</tr>
<tr>
<td>4.10</td>
<td>Summary of Hypothesis Results</td>
<td>49</td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Proposed Model</td>
<td>21</td>
</tr>
<tr>
<td>3.1</td>
<td>Operational Research Framework</td>
<td>25</td>
</tr>
<tr>
<td>4.1</td>
<td>Respondents’ Age</td>
<td>33</td>
</tr>
<tr>
<td>4.2</td>
<td>Participants Educational Level</td>
<td>35</td>
</tr>
<tr>
<td>4.3</td>
<td>Distribution of Administrative and Academic Staff of IT Faculties</td>
<td>36</td>
</tr>
<tr>
<td>4.4</td>
<td>Responses Concerning Corporate Governance</td>
<td>38</td>
</tr>
<tr>
<td>4.5</td>
<td>Responses Concerning Management Support</td>
<td>40</td>
</tr>
<tr>
<td>4.6</td>
<td>Responses Concerning Employee Security Management</td>
<td>42</td>
</tr>
<tr>
<td>4.7</td>
<td>Responses Concerning Cultivation of Information Security</td>
<td>45</td>
</tr>
<tr>
<td>4.8</td>
<td>Cultivating Information Security Culture Model After Analysis</td>
<td>48</td>
</tr>
</tbody>
</table>
LIST OF ABBREVIATIONS

IS - Information Systems
IT - Information Technology
ICT - Information and Communication Technology
HLIs - Higher Learning Institution
CSI - Computer Security Institute
ISRA - 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

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Questionnaire</td>
<td>62</td>
</tr>
<tr>
<td>B</td>
<td>Reliability Cultivation Information Security Culture</td>
<td>69</td>
</tr>
<tr>
<td>C</td>
<td>Reliability Corporate Governance</td>
<td>71</td>
</tr>
<tr>
<td>D</td>
<td>Reliability Management Support</td>
<td>74</td>
</tr>
<tr>
<td>E</td>
<td>Reliability Employee Security Management</td>
<td>77</td>
</tr>
<tr>
<td>F</td>
<td>Regression</td>
<td>80</td>
</tr>
<tr>
<td>G</td>
<td>Frequencies</td>
<td>83</td>
</tr>
<tr>
<td>H</td>
<td>Plagiarism Percentage</td>
<td>85</td>
</tr>
</tbody>
</table>
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


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


