IMPROVING INFORMATION SYSTEM SECURITY BY EVALUATING HUMAN FACTORS

SAEED SOLTANMOHAMMADI

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

Faculty of Computing
Universiti Teknologi Malaysia

August 2013
I dedicated this thesis to my beloved mother, and father for their endless supports and encouragements.
ACKNOWLEDGEMENT

IN THE NAME OF GOD, MOST GRACIOUS, MOST COMPASSIONATE

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

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

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

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

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DECLARATION</td>
<td>iv</td>
</tr>
<tr>
<td></td>
<td>DEDICATION</td>
<td>iv</td>
</tr>
<tr>
<td></td>
<td>ACKNOWLEDGEMENT</td>
<td>iv</td>
</tr>
<tr>
<td></td>
<td>ABSTRACT</td>
<td>v</td>
</tr>
<tr>
<td></td>
<td>ABSTRAK</td>
<td>vi</td>
</tr>
<tr>
<td></td>
<td>TABLE OF CONTENTS</td>
<td>vii</td>
</tr>
<tr>
<td></td>
<td>LIST OF TABLES</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>LIST OF FIGURE</td>
<td>xi</td>
</tr>
<tr>
<td>1</td>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1</td>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>Background of the Study</td>
<td>2</td>
</tr>
<tr>
<td>1.3</td>
<td>Statement of the Problem</td>
<td>3</td>
</tr>
<tr>
<td>1.4</td>
<td>Objectives of the Study</td>
<td>4</td>
</tr>
<tr>
<td>1.5</td>
<td>Significant of the Study</td>
<td>4</td>
</tr>
<tr>
<td>1.6</td>
<td>Scope of the Study</td>
<td>5</td>
</tr>
<tr>
<td>1.7</td>
<td>Organization of Remaining Chapters</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>LITERATURE REVIEW</td>
<td>7</td>
</tr>
<tr>
<td>2.1</td>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>2.2</td>
<td>Information System Security</td>
<td>7</td>
</tr>
<tr>
<td>2.3</td>
<td>System Security Goals</td>
<td>8</td>
</tr>
<tr>
<td>2.4</td>
<td>System Security Threats</td>
<td>9</td>
</tr>
<tr>
<td>2.5</td>
<td>Characteristics of a System Intrusion</td>
<td>10</td>
</tr>
<tr>
<td>2.6</td>
<td>Targeted System Components</td>
<td>10</td>
</tr>
</tbody>
</table>
2.7 Security Implementation

2.8 Role of Human and Organizational Factors in Computer and Information Security

2.9 Information Security and Types of Human Factor Errors

2.10 The Significance of Human Factors in Information Systems Security

2.11 The Contribution of Human Errors in Information Security

2.12 Human Error Models and Concepts

2.12.1 Cognitive Reliability and Error Analysis Method (CREAM)

2.12.2 Situation Awareness (SA)

2.12.3 Generic Error Modeling System

2.13 Categories of Behavior to Distinguish Types of Error

2.14 Classification of Identified Human Error Factors

2.15 Motivational Factors and Information System Security

2.16 Organizational and Information System Security

2.17 Learning and Information System Security

2.18 Proposed Framework

2.19 Summary

3 METHODOLOGY

3.1 Introduction

3.2 Justification of Selected Variables

3.2.1 Organization Factors

3.2.2 Motivational Factors

3.2.3 Learning

3.4 Theoretical Framework

3.5 Hypotheses Development

3.5 Data Collection Method

3.5.1 Primary Data

3.5.2 Target population and sample size

3.6 Instrumentation Design

3.7 Data Analysis Method

3.8 Pilot Study
<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>The Targeted System Components (Nikolakopoulos, 2009)</td>
<td>10</td>
</tr>
<tr>
<td>2.2</td>
<td>Linking the Human Factor (Nikolakopoulos, 2009)</td>
<td>12</td>
</tr>
<tr>
<td>2.3</td>
<td>Relations between CPC score and control modes.</td>
<td>29</td>
</tr>
<tr>
<td>2.4</td>
<td>Dynamics of Generic Error Modeling System (GEMS), (Reason, 1990 and Embrey, 2005)</td>
<td>31</td>
</tr>
<tr>
<td>2.5</td>
<td>Classification of Human Errors (adapted from Embrey, 2005)</td>
<td>33</td>
</tr>
<tr>
<td>2.6</td>
<td>Research Framework</td>
<td>40</td>
</tr>
<tr>
<td>3.1</td>
<td>Research Methodology Framework</td>
<td>47</td>
</tr>
<tr>
<td>3.2</td>
<td>Theoretical Framework</td>
<td>48</td>
</tr>
<tr>
<td>4.1</td>
<td>Frequency of Age</td>
<td>55</td>
</tr>
<tr>
<td>4.2</td>
<td>Gender</td>
<td>56</td>
</tr>
<tr>
<td>4.3</td>
<td>Frequency of Qualification of Employees</td>
<td>57</td>
</tr>
<tr>
<td>4.4</td>
<td>Race</td>
<td>57</td>
</tr>
<tr>
<td>4.5</td>
<td>Frequency of experience in healthcare</td>
<td>60</td>
</tr>
<tr>
<td>4.6</td>
<td>Frequency of computer experience</td>
<td>61</td>
</tr>
<tr>
<td>6.1</td>
<td>Design of a new framework</td>
<td>80</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>The contribution of Human Errors in Information Security. (Ahmed et al, 2012)</td>
<td>26</td>
</tr>
<tr>
<td>2.2</td>
<td>Control modes and probability interval (He et.al, 2008)</td>
<td>29</td>
</tr>
<tr>
<td>2.3</td>
<td>Contrast of two extreme cases, knowledge-based mode and skill-based mode</td>
<td>35</td>
</tr>
<tr>
<td>2.4</td>
<td>Summery of Reviewed Models. (Fotta et al., 2005)</td>
<td>35</td>
</tr>
<tr>
<td>2.5</td>
<td>Previous Research on Human Errors</td>
<td>37</td>
</tr>
<tr>
<td>3.1</td>
<td>Independent and Dependent Variables</td>
<td>49</td>
</tr>
<tr>
<td>3.2</td>
<td>Questionnaires’ Distribution</td>
<td>50</td>
</tr>
<tr>
<td>3.3</td>
<td>Rating scale (5point Likert scale)</td>
<td>51</td>
</tr>
<tr>
<td>3.4</td>
<td>Reliability for 150 data</td>
<td>52</td>
</tr>
<tr>
<td>4.1</td>
<td>Age</td>
<td>55</td>
</tr>
<tr>
<td>4.2</td>
<td>Gender</td>
<td>56</td>
</tr>
<tr>
<td>4.3</td>
<td>Qualification</td>
<td>57</td>
</tr>
<tr>
<td>4.4</td>
<td>Race</td>
<td>58</td>
</tr>
<tr>
<td>4.5</td>
<td>Experience in healthcare</td>
<td>59</td>
</tr>
<tr>
<td>4.6</td>
<td>Computer experience</td>
<td>60</td>
</tr>
<tr>
<td>4.7</td>
<td>Mean Analysis</td>
<td>62</td>
</tr>
<tr>
<td>4.8</td>
<td>Tests of Normality</td>
<td>63</td>
</tr>
<tr>
<td>4.9</td>
<td>Internal Consistency</td>
<td>64</td>
</tr>
<tr>
<td>4.10</td>
<td>Reliability for 150 data</td>
<td>64</td>
</tr>
<tr>
<td>4.11</td>
<td>Pearson Correlations of independent variables</td>
<td>65</td>
</tr>
<tr>
<td>4.12</td>
<td>Pearson Correlations of Sub independent variables</td>
<td>66</td>
</tr>
<tr>
<td>4.13</td>
<td>Multiple Regression Analysis</td>
<td>67</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>4.14</td>
<td>Correlations summary of independent variables</td>
<td>69</td>
</tr>
<tr>
<td>4.15</td>
<td>Correlations summary of sub independent variables</td>
<td>69</td>
</tr>
<tr>
<td>4.16</td>
<td>Summary of Hypothesis Testing</td>
<td>70</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Introduction

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

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

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

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

1.3 Statement of the Problem

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

Since numerous organizations use and apply advanced technologies in their security systems such as smart card and biometrics, external threats are not the main concerns in information security (Kreicberge, 2010 and Leach, 2003). As Leach (2003) stated, the main concerns are related to internal threats such as users' carelessness, errors and omissions which are all caused by internal factors an categorized as poor users’ behaviors. According to some studies, in so many security breaches employees in an organization can be guilty intentionally or unintentionally (Kreicberge, 2010; Siponen et al., 2010). Employees' guilty role is something that is an internal threat. As Boujettif and Wang (2010) reported 4 out of 5 security incidents in organizations are caused by internal threats. Some researches in Malaysia support this fact. For example, Human error is one of main internal threats in applying Health Information System in Malaysia (Samy, 2010; Humaidi, and Balakrishnan, 2013).
1.4 Objectives of the Study

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

1.5 Significant of the Study

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

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

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

1.6 Scope of the Study

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

1.7 Organization of Remaining Chapters

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

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

Chapter 3 – Hypothesis Developing and Methodology: This chapter attempts to generate an appropriate conceptual frame work for this study to explain the relationship between the variables (independent and dependent). For this purpose all variables are justified based on literature and current conditions. Besides, it describes method of data collecting, screening and analyzing.
Chapter 4 – Data Analysis: This chapter covers the quantitative analysis, research design and the suitable methodology in relation to impact of mentioned independent variables on Information System Security. Besides, it explains the sample of study, data collection, different variables for developed model, and the statistical tool applied in this research. Thus, the result will provide in terms of descriptive statistics, and Regression analysis.

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

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


