

## CHAPTER 8: CONCLUSION

This chapter summarizes the research project, restates the research problem and lists the research questions. Contributions of the current study to existing knowledge are examined. Implications for academia and for practice are provided, followed by limitations of the research and recommendations for future research.

### 8.1 Overview

Information security and its management are concerned with people, processes and technology. Whilst the technology itself is relatively objective by nature, the people and processes are influenced by the environment in which they operate. People and processes are influenced by human behavior which might in turn substantially influence the management of information security. Numerous academics have argued that the human dimension in information security forms its weakest link (S. M. Alfawaz, 2011; AlKalbani et al., 2015; Da Veiga & Eloff, 2010; Kunnathur, 2015). Thus, the creation of a security culture is essential and inevitable for organizations to enhance the effectiveness of managing information security (S. M. Alfawaz, 2011; M. A. Alnatheer, 2014; Knapp & Ferrante, 2014). The significance of the current study lies in identifying and exploring successful socio-technical factors that influence the effectiveness of information security and develop a security framework to improve the effectiveness of e-government security in developing country. The current study was one of the earliest in the information security area from the socio-technical aspect to develop a reliable and valid security culture measurement framework as a major contribution to this area of research.

An extensive literature review revealed that there is a resulting lack of attention in the open literature on socio-technical factors and how these factors relate to generic attitudes towards information security and its management. This lead to the research problem that this study addresses:

The research problem addressed in the current study was:

*What socio-technical elements need to be addressed or managed to develop and deploy an effective information security to help the government's top management in ensuring the security of e- government environment?*

In particular, the variety of perception and behavior of people that may make e-government services insecure needs to be addressed. To address the research problem, an exploratory review analysis of literature was conducted in order to identify successful socio-technical factors that influence the effectiveness of information security. The outcome of the literature review revealed that lack of a socio-technical security factors is a major concern in security frameworks and models have been developed and proposed for developing countries e-government. Quantitative instruments were used to develop and validate the framework. To address the research problem, four research questions were formed, which were:

**RQ1:** *What are the socio-technical factors that affect the security of e-government?*

A comprehensive review was conducted of information security current literature from socio-technical aspect. The purpose was to identify a set of candidates for building a conceptual framework. To answer this question, this study explored and identified successful social-technical factors related to the information security in organizations. It explored these factors based on literature view, documents, and expert's perspective, and grounded on the Socio-Technical approach, Security By Consensus (SBC) model, and adapting earlier work (Kankanhalli et al., 2003; Straub Jr, 1990), to address concerns about security effectiveness. The findings, factors influencing security culture were found to be: Legal & law, Compliance, Ethical Conduct, Security Policy, Security Awareness, Security Training, Top Management Support, IS structure. The importance of these factors on security culture creation and improving the effectiveness of information security was discussed in various literatures.

*RQ2. How significant are the various factors in influencing information security of e-government?*

Quantitative analysis of the organizations' employees' experiences were analyzed and discussed to examine the influence of these factors on the organization security. After identifying and investigating the factors, the framework was developed for improving the effectiveness of e-government security.

*RQ3: How the proposed framework can be validated?*

This research question was aimed to assess and validates the security culture framework. Structural Equation Modeling (SEM) was employed as the technique for evaluating and validating the relationships between the frameworks constructs which presented SEM components of a measurement framework. In addition, it was done to gain an initial understanding of the relationship between socio-technical factors that influence security culture to improve the effectiveness of information security in e-government.

The proposed framework was developed based on the outcome of the review of literature and data analysis. Afterwards, the proposed framework was tested using SEM technique throughout chapter 6. The research data in this study offered a nomological validity to the conceptualization of a security culture measurement framework. The findings in this study supported the assertion that factors influencing the effectiveness of the information security consisted of eight factors: Legal & law, Compliance, Ethical Conduct, Security Policy, Security Awareness, Security Training, Top Management Support, IS structure, mediated by security culture.

The security culture measurement framework instruments that were demonstrated produced excellent reliability estimates, and evidence also supported their content validity, discriminant validity, convergent validity, and nomological validity. The findings indicated that factors influence security culture are positively associated with Legal & law, Compliance, Ethical Conduct, Security Policy, Security Awareness, Security Training, Top Management Support, IS structure, and all of these factors have positive influence on security effectiveness and mediated by Security culture. In addition,

positive correlations, consistent with theoretical predictions, were obtained between factors influencing security to improve the effectiveness of information security for e-government. These correlations provide further support to the nomological validity of the information security culture measurement framework. The outcome of the current study consolidates security culture literature and could serve as a basis for future inquiries in this area. However, certainly the current study cannot claim that the framework is the final word on information security. Therefore, more work in the future is expected.

## **8.2 Research Outcome Contributions**

The majority of past research on information security has provided a great deal of knowledge concerning the current state of the study area and important critical aspects affecting the creation of information security effectiveness. However, the socio-technical factors' influence or drive security effectiveness have not been substantially examined and particularly not from an empirical standpoint. In an attempt to fill the research gap and to contribute to the existing body of knowledge, this research developed an information security culture measurement framework. The study framework is strongly supported by empirical evidence using quantitative assessment.

### **8.2.1 Theoretical Contribution**

#### **8.2.1.1 Framework**

This research discussed the socio-technical factors and the importance of these factors to create information security culture. This includes providing an initial understanding of the relationship between factors influencing security effectiveness - areas in which no prior academic literature had addressed the relationship specifically in Malaysian context. In order to fill an existing gap in the literature, the current study developed an information security measurement framework which was designed to assist in better understanding the

relationship between these factors and the influencing of these factors to improve the effectiveness of information security. A better understanding of such relationships can provide a better picture of how to develop an effective information security in more effectively in Malaysian e-government sector. This understanding will improve the understanding of securing e-government amongst information security practitioners.

#### **8.2.1.2 Methodology**

By using quantitative survey, the measurement items of the study constructs were identified by rigorous statistical testing to check validity and reliability. The results showed that there is a high degree of construct validity, reliability, and discriminant validity for each of the constructs within the framework. In addition, satisfactory fit indices with significant pathways in the hypothesized direction between the theorized constructs were evident. This methodology explains how the validate instrument and framework were developed to assess the information security culture framework.

#### **8.2.2 Industry Contribution**

##### **8.2.2.1 Information Security Community**

This study is a significant endeavor to address the human risk of e-government. Previously, security emphasis was made to the technological solutions. With this research, it explains the implications of culture on information security. It provides insights to how information security should be done in an effective manner using a socio-technical approach. It examined socio-technical factors to determine how it affects information security. This study indicates that creating security cultural is significant to improve the effectiveness of information security.

### 8.2.2.2 E-government Community

The outcome of this research is to provide the information security culture framework for e-government environment. The proposed framework can be used as a guide to direct e-government practitioners to focus on information security from different angle – socio-technical perspectives. It would be beneficial to the e-government practitioners to classify the suitable controls and solution to increase the awareness of their employees towards security.

### 8.2.2.3 Other E-Services Community

Although the validity framework of this research was tested on e-government environment, it is flexible enough to be adapted to minor technical changes that may occur in the future. Moreover, it can be used for other e-services such as e-learning, e-health, and e-commerce. In addition, the research framework was tested in Malaysian environment. However, it is applicable far beyond this geographical and contextual domain. It can be implemented in different countries for use in studying any e-government systems.

In addition, the study's contributions include:

- The current study underpinned or identified what are successful socio-technical factors that influence the effectiveness of information security through an extensive review of the literature. Being able to understand critical socio-technical factors that constitute or reflect information security is a major challenge that required a synthesis of the literature findings. This will serve as a foundation for an early understanding of information security creation. This constitution of information security reflective behavior is considered very important contribution to the information security research area since there is otherwise a clear need to identify these factors. This work substantiates the claim that factors influencing

information security effectiveness are: Legal & law, Compliance, Ethical Conduct, Security culture, Security Policy, Security Awareness, Security Training, Top Management Support, IS structure. So if individuals within an organizational setting demonstrate high awareness of information security practices and procedures by good training program, follow the security policy, and feel the responsibility legally and ethically for protecting information security with top management support, a security culture is most likely to be created and the effectiveness of the security improved.

- The outcome of the current study was an information security culture measurement framework which was found to be reliable through Cronbach's alpha and item total correlation. The information security culture measurement framework was the first study, as far as the researcher is aware of, to empirically validate the conceptualization of factors pertaining to security effectiveness. Additionally, the current study is one of the earliest studies to validate the security culture measurement framework with various validation techniques such as exploratory factor analysis to indicate the relationship between constructs and confirmatory factor analysis. The final outcomes provided robust structures that serve as a basis for subsequent framework assessment. The framework was refined and then the first study in the information security effectiveness area assessed using advanced statistical instruments such as SEM techniques to ensure the nomological validity of the research framework. In addition, to establish the full nomological validity of the framework, a mediation check was performed. A check that, by necessity, must be done in stages, and confirming the results through Bootstrapping procedure. This is a thorough approach to assessing the framework.

### **8.3 Implications**

There are two implications (Research and practice) for the current study.

### 8.3.1 Implications for Research

It is essential to assess and understand the existence of important factors that influence information security in order to create a security culture to improve the effectiveness of information security. To achieve this goal, the current study developed an information security culture framework in order to understand security culture creation in Malaysian e-government sector. The current study's major beneficial contribution lies in providing a reliable and valid the socio-technical security framework. Secondly, the framework will also initially assist in assessing the relationship between successful socio-technical factors that influence security effectiveness. The following headings summarize the research implications for the current study.

- The current study assists academic researchers to identify research gaps in the information security field from socio-technical aspect, including identifying further empirical research needed in this area. Therefore, the current study assists in filling a major gap in the area of information security from socio-technical aspect. This includes developing a reliable and valid information security culture framework that could be replicated in other environment. Furthermore,
- From a methodological standpoint, the current study has a major contribution to information system security research. It illustrates that a deductive method research design using a quantitative methods can be conducted in information security. The current study provides exploratory review of literature that could assist in developing an information security culture measurement framework in developing countries such as Malaysia. The methodological contribution is provided through an operationalisation of information security culture measurement framework constructs. The current study demonstrates that quantitative assessment was valuable validating the nomological net of the developed framework. Additionally, the quantitative assessment assists in exploring the initial understanding of the relationship between framework constructs. This methodology provides a useful tool to assist researchers in carrying out empirical studies associated with information security.

### 8.3.2 Implications for Practice

The current study presents a quantitative assessment that can be used by information security managers and practitioners to measure security culture and the usefulness for creating a security culture to improve the effectiveness of the information security. The instruments presented were designed with academic rigor and tested across multiple phases with empirical data. The research framework was statistically tested for validity and reliability with 312 participants from Public Service Department Malaysia (JPA). The research framework offers a number of observations that can guide managers in organizations to enhance the creation of a security culture to improve the effectiveness of the information security. The observations are:

- The current study assists information security managers in developing important aspects of information security that will lead to the creation of a security culture that improve the effectiveness of the information security. The research framework provides management with the means to implement effective information security management approaches. These approaches will provide a single point of reference for managing information security to inculcate an acceptable level of security culture. These approaches include providing guides to managers in understanding the importance of top management support for the creation of security culture, in particular by enforcing and communicating the security policy. The presence of these factors substantially positively influences the creation of a security culture.
- This research helped in minimizing the threats that the behaviors of employees pose to the protection of an organization's information assets. The information security culture measurement framework facilitates the understanding of information security culture and of elements that could reinforce the security culture. By understanding these factors management can assist in directing the interaction of humans with information security in order to contribute to the protection of information assets.

## 8.4 Limitations

The following points summarize several possible limitations of the current study:

- The framework testing results had not taken into considerations for the following control variables (which may produce different statistic results): education level, job title, and job experience.
- Time constrains was the major limiting factor of this research work, the empirical study in this research was limited to only one of the developing countries (Malaysia), Additionally, although the choice of a quantitative survey method in this research was adequate in obtaining data to answer the research questions, future research may employ qualitative research design involving case studies or observations. Integrative triangulation approach is another possible method that can be used by combining both quantitative and qualitative design involving in-depth interviews with top-level management.
- The finalized framework had not taken into considerations for the following factors such as risk assessment, assist management, and change management (which may have influence on information security culture).

## 8.5 Future Research

Future research may include the following:

- Understanding information security culture from different perspective such as what factors could influence security culture to improve the effectiveness of information security in other environment.
- Expansion of our framework to other countries in the region.
- Including other socio-technical factors such as risk assessment, assist management, and change management in the proposed framework and investigating the influence of these factors on security culture to improve the effectiveness of information security.
- The study could also investigate the effects of adopting cloud computing security services in the studied environment.

- Conducting a comparative analysis between Malaysian e-government and other developed countries such as Australia or the USA.
- Replicating the study in different environments (Europe, North America and Australia) with different demographic groups.

## 8.6 Conclusion

This research is a study that looks at security in e-services specifically on e-government. It has uniquely highlighted the cultural view of people towards information security.

The research study was conducted in response to the need for more empirical studies that focus on the development of information security culture measurement framework. As a result, an information security culture framework has been developed to help e-government providers to manage the information security issue. To achieve the aim of the study, an information security culture measurement framework comprising factors influencing security culture to improve the effectiveness of the information security was developed based on review of literature and data analysis findings. Then the framework was assessed and refined using a series of quantitative techniques, specifically Exploratory Factor Analysis (EFA), Confirmatory Factor Analysis (CFA), Structural Equation Modeling (SEM), and nomological validity. These techniques were conducted based on the data obtained from a questionnaire survey of Malaysian e-government sector employees. The current study contributed to existing knowledge by providing a valid and reliable information security culture measurement framework, in addition to providing an initial understanding of the relationship between socio-technical factors influencing security culture to improve the effectiveness of e-government information security. The current study provided practical implications to Malaysian e-government by offering a framework that could explain and provide information about a security culture measurement framework. The framework could improve security effectiveness for Malaysian e-government sector. This research has emphasized that information security is the responsibility of everyone and the way of enforcing this is by addressing cultural views.

Finally, the current study closed with future work recommendations that may assist researchers to enhance and extend the findings of this study.

UNIVERSITI SAINS ISLAM MALAYSIA  
جامعة العلوم الإسلامية  
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA