CHAPTER 1: INTRODUCTION

1.1 Research Background

Invention and existence of Internet in today's information rich societies has become an essential channel for dissemination of information and various services. Many electronic services such as E-Learning, E-Commerce, E-Business, E-Banking and E-Government have become possible with this information and communication technology (ICT) innovation. E-Government, to put in simple words, is the use of ICT to enhance the delivery of information and services to others and to improve internal government procedures. There are many benefits of E-Government in transforming traditional government into effective e-government, such as cost effective delivery of services, integration of services, reduction in administrative costs, a single integrated view of citizens across all government services and faster adaptation to meet resident's needs (Karunasena & Deng, 2012). Due to such advantages, E-Government has become a global trend and an important tool for innovation and government reforms. E-government projects were launched since the late 1990s (Abdallah & Fan, 2012). Since then, governments across the world are grasping the digital transformation to broaden services for their citizens (Markaki et al., 2010). Over the past decade, many governments throughout the world have built up their efforts to improve the efficiency of public services through ICT (Weerakkody et al., 2012).

E-Government has many benefits to our modern world through services provided over the internet which include- (1) increased transparency, (2) enhanced efficiency and quality, (3) full access to information and individual services (Alshboul, 2012) and (4) opportunities for citizens to interact and receive services from public organizations 24 hours a day, seven days a week (24/7 – basis) (Waziri & Yonah, 2014). However, the ability to achieve full benefits of e-government in developing countries is limited due to various legal, political, economic and social issues (Gebba & Zakaria, 2012).

E-Government projects face many challenges that may lead to failure of e-government implementation. According to Heeks (2003), over 60% of all E-government projects have been unsuccessful. Therefore, there is a need to look at the reasons of e-government implementation failure (Al-Azri et al., 2010). Of the reasons, information security is identified as one of the requirements for the successful e-Government implementation (Shayan et al., 2010).

As a result of growth in media communication and transmission of information, the need of information security has risen to high levels. Rapid development of e-Government has exposed critical public information to the possibility of cybercrime (AlKalbani et al., 2015). The findings of various national surveys confirm a high number of cyber attacks against the information resources of such organizations (Harris et al., 2014; S.Corporation, 2014) (more details in next paragraph). Therefore, the need to secure the information and minimize the risk is becoming more important than ever before and information security has become a critical issue that needs to be adequately addressed during e-Government planning and implementation processes.

The term 'information security' is defined as "protection of information from threats, to minimize the risk and maximize return on investments and business opportunities, to ensure business continuity" (Mohd Alwi & Fan, 2010). It is quite important for any E-government services to maintain a sufficient level of security for protecting personnel information of millions of citizens who utilize such services. In the world of cyber warfare, while government websites are becoming increasingly prone to numerous threats which make the securing sensitive government data a great challenge for government organizations, increased attention is also given to the security related issues of these websites to ensure the adequate protection of their sensitive information (Saint-Germain, 2005).

As noted by Raman and Wei (1992) and Ruighaver et al. (2007), the success of information security management practices is affected by the environment in which it is managed as procedural, contextual, and political factors are interrelated where

explanations for outcomes are sought. Hence, the contextual pressures and constraints of the environment have an impact on the success of ISM and the knowledge Management (KM) systems.

In terms of information security, Sveen et al. (2007) distinguished between securing knowledge assets and managing security knowledge. Securing the knowledge asset may be thought of as ensuring its correct and appropriate use in the mission of the owner of the information. On the other hand, managing security knowledge concerns the collection, validation, and application of security-related information for the benefit of the firm. They argue that it is important to take into consideration the effects of organizational and individual factors such as organizational culture in support of secure knowledge management systems.

Culture has been identified as an underlying determinant of individuals' behavior Mohannak and Hutchings (2007) stated that some activities and institutions in the KM process are more directly steered by local cultures. They concluded that the cultural backgrounds of people in developing countries often reduce the effectiveness of certain activities such as knowledge sharing, which is not the case in developed countries. This cultural influence can result in undesirable design and reality gaps, which tend to lead to under performing systems (Heeks, 2002, 2003). Mohannak and Hutchings (2007) also argue that any cross-cultural and institutional framework for understanding the KM style should include at least three dimensions: contextual factors, the participants, and the KM process. The cultural influence on security aspect of knowledge and information sharing will be investigated as a critical factor in effective information security culture development.

Several studies have confirmed that the problem of electronic data theft is growing. A 2014 Symantec report noted that there was an increase in number of large data breaches, and a dramatic five-fold increase in number of identities exposed over a single year

(S.Corporation, 2014). In October 2013, all open data platforms in US federal government, including Data.gov were considered non-essential services and were shutdown (Baker, 2013). In September 2014, Home Depot's corporate network was penetrated and over 56 million credit card numbers were acquired (B. Chen, 2014; Krebs, 2014). In February 2015, the second largest health insurer in the United States, Anthem Inc., was attacked, and 80 million records containing personal information were stolen (Mathews & Yadron, 2015). Thus, such failure to protect and secure these services can be hazardous not only for government and business organizations but also for the public at large. Therefore, every attempt must be made to ensure the security of these services provided by the government and to earn the trust of the beneficiaries of these services. It should be remembered that e-government does contribute positively; at the same time, also generates threats to the country if not properly managed. The factors that may threaten e-government information security are from internal and external government system. Internal threats are mainly from human factors within the system while external threats are from the physical environmental factors and human factors beyond the system (Zhao, 2011).

Most of the research on information security so far has focused on technical solutions (M. T. Siponen & Oinas-Kukkonen, 2007). It has been reported that security threats could result from technical issues such as vulnerability caused by poor system design, implementation, configuration, integration and maintenance, and socio-technical issues which may result from lack of legal, cultural and ethical, operational and procedural guidelines, administrative and managerial policies (M. A. Alnatheer, 2014; Gil-García & Pardo, 2005; S. Kowalski, 1994; Michael et al., 2007). Studies have also shown a myriad of problems facing the organization in their effort to implement security program effectively from social-technical aspects (S. M. Alfawaz, 2011; Tarimo et al., 2006). As security issues are not only due to technical problem, overall studies show that the lack of security is the most common problem faced by many e-government projects, there is lack of discussion on information security from socio-technical perspective for e-government. As a result, the socio-technical attention to information security has been low compared

to technical issues, therefore in this research; the researcher proposes an e-government security framework, which consists of technical and socio-technical aspects in e-government environment.

Many researches findings have concluded that a universal model or framework for securing e-government, which can be applicable for all countries is not rational and practical idea due to differences in contexts and set of security requirements (Abdallah & Fan, 2012; Al-Shafi & Weerakkody, 2010). However, most of the literature adopts a Western culture or industrialized perspective. When the context of information security management is a developing or non-Western or non-industrialized culture, this literature may not be applicable (S. M. Alfawaz, 2011). Literature has pointed out that people's behavior required to be addressed to control the information security threats. Therefore the security issues related to the people and processes components of information security need to be focused. This leads to the need for the socio-technical approach of focus in these issues.

1.2 Research Motivations And Problem Area

Information security has become a critical issue that needs to be adequately addressed in e-Government development. Cyber security risks are prevalent in today's information age, and new cyber incidents appear regularly in the news. In this respect, the Global State of Information Security® Survey 2016 showed that the rate of detected security incidents in 2015 has increased 38% over 2014 (Coopers, 2016). Thus, as the number of e-government services introduced to the user increases, a higher level of e-government security is required (Ibrahim & Hamid, 2013). The existing studies have concluded that:

- There are more focus in developing technical security than socio-technical security (Salih et al., 2013).
- Socio-technical issues are as important as technical issues (Dhillon et al., 2007; Shaaban, 2014).

- Many incidents of information security are caused by human behavior, rather than by technical failures (M. A. Alnatheer, 2012; Beautement et al., 2009).
- Survey conducted by The Global State of Information Security Briney (Coopers, 2016) showed that most of security problems were caused by the negligence of people, rather by attack events. Employees were the most-cited offenders of incidents. Thus, people posed the most risk to the organization, not technology.

Many researchers have emphasized that different information security components such as human factors, organizational factors, and technical factors can be used to provide a comprehensive information security effectiveness model or framework (AlKalbani et al., 2014; Brady, 2011; D'Arcy & Hovav, 2009; Da Veiga & Eloff, 2010; Herath & Rao, 2009; Kankanhalli et al., 2003; Knapp & Ferrante, 2014; Narain Singh et al., 2014; Veiga & Eloff, 2007). There is clear need to focuses on the socio-technical approach to improve the e-government security. This is a very topical issue nowadays which is not yet widely addressed (S. M. Alfawaz, 2011). However, findings of the analysis of different models and frameworks on information security related works have shown that they lack socio-technical security elements. Particularly, with respect to developing countries, 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 has led to the research problem that this study addresses:

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.

1.3 Research Aims

The aim of the study is to develop an information security culture framework for e-government in developing countries, in order to facilitate government organizations in effectively and appropriately securing e-government services.

1.4 Research Questions

The following research questions have guided the study.

RQ 1: What are the socio-technical factors that affect the security of e-government?

This research question aimed to explore and identify socio-technical factors related to information security in different government organizations

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 an organization security. After identifying and investigating the factors, the framework was developed for securing e-government.

RQ 3: How the proposed framework can be validated?

This research question aimed to assess and validate the framework.

1.5 Research Objectives

1. To identify the socio-technical factors that affects the information security of e-government.
2. To develop information security culture framework for e-government.
3. To validate the framework.

1.6 Scope Of The Research

This study is limited to the government sectors in developing country, practically in Malaysian context. In addition, the study has been conducted using the existing knowledge and focuses on three main areas such as information security, e-government and Malaysian context. The intersection of these areas is the focus of this study - the e-government security in Malaysia, using the socio-technical approach.

Malaysian context was selected due to three reasons. Firstly, the author is research student in Malaysia which made the data collection easier. Secondly, Malaysia aspires to be a developed country by the year 2020 comprising of a community that has abundance of information and knowledge in line with the country's National Vision Policy. One of the major steps undertaken is the conceptualization of the Multimedia Super Corridor Malaysia (MSC Malaysia) project. Under the project, electronic government (e-government) has been identified as a flagship to be developed and implemented by the Malaysian government. Furthermore, according to Malaysian national agency ("CyberSecurity Malaysia," 2015) in Quarter 2 (Q2) 2015 the cyber security incidents increase about 4.47% of the total incidents compared to Quarter 1 (Q1) 2015, due to Malaysia's interest and continued effort in e-government implementation, where the data collection and findings may contribute to e-government effort in the country. Thirdly, due to lack of available research studies on this topic in Malaysian context.

1.7 Research Methodology

This research is carried out to propose an effective way to facilitate e-government organizations in effectively and appropriately securing e-government services, by developing an information Security culture Framework. With such purpose, this research used deductive approach to suit in the quantitative research perspective to meet the research objectives. The research methodology is divided into four phases: Planning phase, Data Collection and Analysis Phase, Framework development Phase and

Discussion and Conclusion Phase. Figure 1.1 outlines the overall of four main research methodology phases.

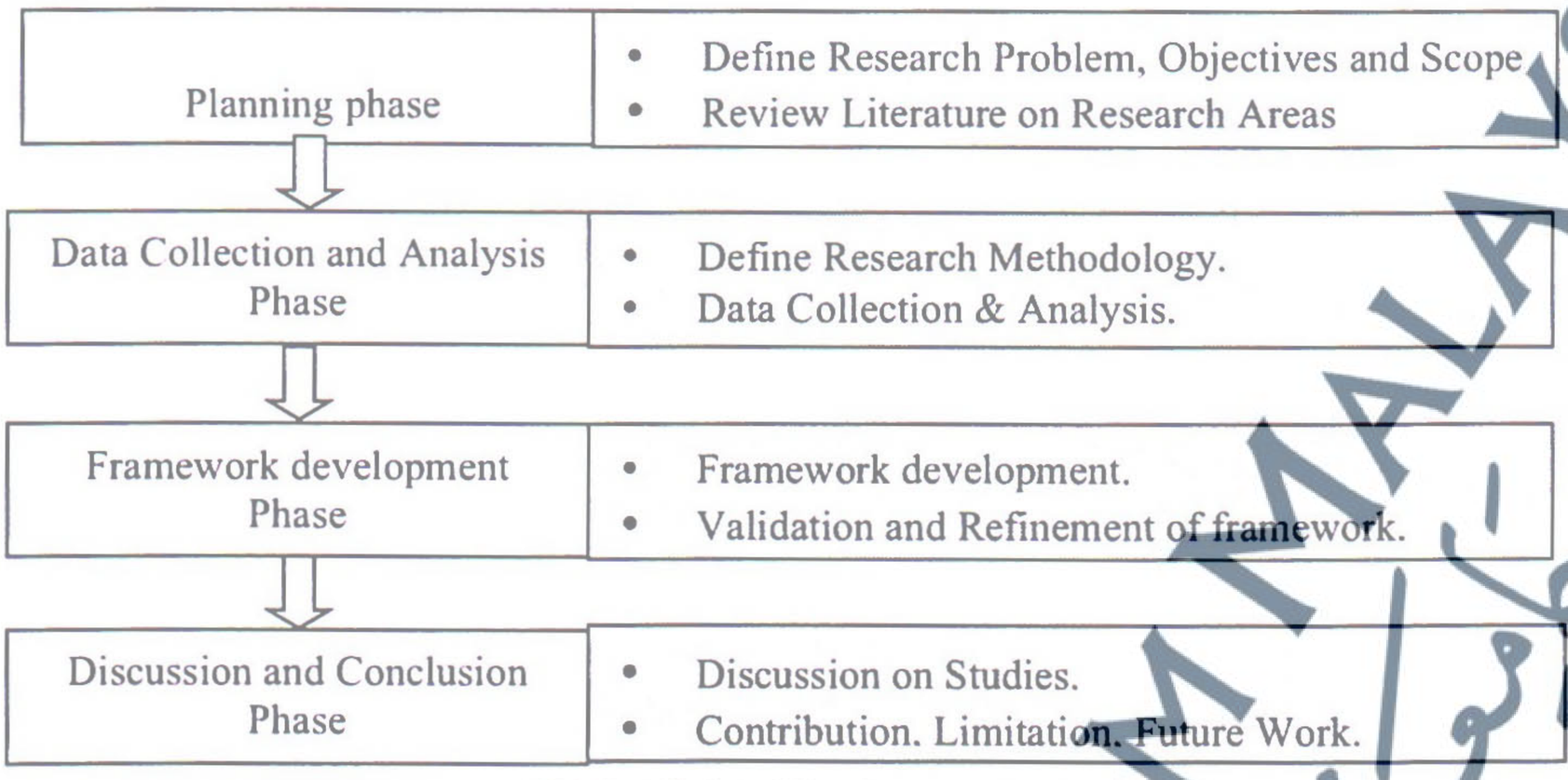

FIGURE 1.1: The Research Methodology

1.7.1 Planning Phase

The Planning Phase studies the research topic and finds the literature gap. In this phase, the research problem, objective and scope were initially defined. In order to further understand the topic, the main research areas - information security, e-government. The literature review has revealed that little research has been conducted in securing e-government in developing countries. At the end of the review, gaps and unknown situations are found. The output of this phase has lead to the definition of research requirement.

1.7.2 Data Collection and Analysis Phase

This research is conducted with a quantitative research strategy using questionnaire for data collection. Systematic approach and extensive search on secondary data resources was conducted to identified the socio-technical factors and develop survey questions. Sense E-Government is one of the leading flagships applications of the Public Service Department Malaysia (JPA) project, the survey-based used to collect data from (JPA), and 312 questionnaires were collected. Authority and uses a combination of statistical

techniques, such as exploratory factor analysis (EFA), confirmatory factor analysis (CFA), and structural equation modeling (SEM).

1.7.3 Framework Development Phase

In this phase, the security culture framework for e-government developed and validation activity is carried out. Expert reviews on the research findings and framework were performed. The open-ended questionnaire was used to extract the experts' opinion regarding the framework potential and applicability of the research findings. Description on the experts review is in Chapter 6.

1.7.4 Discussion and Conclusion Phase

The final phase reflects on the development as a part of academic research. The discussion addresses the aim and the objectives, while the conclusion summarizes the research contribution and future work. This phase can be found in Chapter 7 and Chapter 8.

1.8 Research Contribution

This research may contribute to three communities as discuss below.

1.8.1 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 into 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 culture is significant to improve the effectiveness of information security.

1.8.2 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 e-government practitioners to classify the suitable controls and solution to increase the awareness of their employees towards security.

1.8.3 Other E-Services Community

Although the validity framework of this research was tested on e-government environment, 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 can be applicable far beyond this geographical and contextual domain. It can be implemented in different countries for use in studying any e-government systems.

1.9 Thesis Structure

The thesis is organized into eight chapters:

Chapter One- Introduction: this chapter presents the research background, research aim, objectives, and research questions. In addition, it briefs on the research methodology and contribution.

Chapter Two- Literature Review: This chapter reviews the research related literature on e-government and information security. The survey includes review on socio-technical approach and information security culture etc. The literature gap is also summarized here.

Chapter Three- Methodology: The research methodology is presented in this chapter. The research perspectives, research design and research processes are also discussed.

Chapter Four-Data Analysis and Results: This chapter presents the data analysis, the detailed results of the descriptive statistics analysis subsequent multivariate statistical analysis such as Exploratory Factor Analysis (EFA), Confirmatory Factor Analysis (CFA) based on the questionnaire survey of Malaysian organizations.

Chapter Five- Framework Development: This chapter explains the development of the security culture framework for e-government framework.

Chapter Six-Framework Validation: This chapter presents the framework validation process, the framework validation was sequentially undertaken based on the results of the above measurement scale analysis. This chapter begins with SEM overviews using Covariance-based method such as Analysis of Moment Structures (AMOS). And presents the feedback obtained from the experts.

Chapter Seven- Discussions: This chapter presents the research findings as achievement of the research aim and objectives, discusses the quantitative study findings, and hypotheses testresults. In addition, the framework refinement presented.

Chapter Eight-Conclusion: This chapter presents the summary of research process and findings. In addition, the contributions, research limitations and future work are provided. The thesis ends with the research conclusion.