CHAPTER5: FRAMEWORK DEVELOPMENT

This chapter aimed to describe the development of the information security culture framework for securing e-government services that emerged from existing theory, the literature review findings, and data analysis results. The socio-technical factors influencing security and the development of a specification of the framework are also discussed.

5.1 Socio-Technical Factors

Since the socio-technical security area is considered in the early stages of development, the literature analysis were undertaken in related area to socio-technical security focusing on information security management. This is because the existence of socio-technical security is well considered as part of effective security management practices. As a result of an extensive literature review, the socio-technical factors that may influence information security were identified as follow:

- **Legal & law**

The lack of legal development is one of the information security challenges in an organization. Legislation and laws should provide the basis for ensuring an adequate level of compliance to international regulations and laws as well as giving internal direction. On a legal level, it is important to increase the level of harmonization of data protection legislation, to ensure a coherent application of this legislation and to ensure a high level of enforcement.

- **Compliance**

It is widely recognized that many security incidents are caused by human behavior, rather than by technical failures. Security breaches perpetrated by employees were accidental. This demonstrates a negligence or ignorance of the security policies of the organization. Employees often are not aware of the security consequences of their actions and do not understand enough about the impact of their security decisions. This can be resolved if a clear vision from senior management is presented to influence employees' behavior to protect the organization's information assets through compliance with the security policy.

- **Ethical Conduct**

Ethical conduct can be used to control the behavior of employees and establish 'moral' codes for the company. Codes of ethics and conduct "facilitate responsible security awareness, as users are held personally responsible for ensuring sound security practices are implemented, reducing the security risks" Therefore, information security ethics play a major role in addressing security problems.

- **Security culture**

Security culture is a set of information security characteristics that the assumption about what is acceptable and what is not in relation to information security, the assumption about what information security behavior is encouraged and what is not, and the way people behave towards information security in the organization.

- **Security Policy**

Security policy is the foundation for any security regime and specifies the strategies behind an organization's information security approach by a written document, directly linked to the overall policies of the organization. The primary objective of an information

security policy is to define the user's (i.e., employee's) rights and responsibilities in an organization.

- **Security Awareness**

Information Security Forum (ISF) defines security awareness as:

The extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly. The importance of security awareness is a vital part of protecting information security and creating an effective approach to manage information security.

- **Security Training**

There is a strong belief that security training is the key to improve information security. Without security training programs, people will always be the weakest link and the organization will still be at risk. Organizations need to ensure that an information security culture is inculcated through training, education and awareness raising, in order to minimize risks to information assets. The proper training and education help change people's mindsets and behaviors toward security.

- **Top Management Support**

Executive support can be helpful in promoting an effective information security program. Top management support refers to the degree to which senior leadership understands the importance of the information security function and the extent to which it is involved in information security activities.

- **Information security structures**

Information security systems are mostly defined as systems that protect information assets from harm or misuse. Traditionally the main information security services are the preservation of confidentiality, integrity and availability of information. Security mechanisms are the technologies that provide the security services; for example digital signatures, firewalls, antivirus, intrusion detection, and access control mechanisms. These types of technologies can help in providing confidentiality, integrity, authentication, and non-repudiation services for organizations' information security system.

5.2 The Framework Development

The process involved utilizing suitable research approaches, methods and theoretical foundation from the existing theories in information security and e-government. These includes soft systems methodology (Checkland & Scholes, 1990), socio-technical modeling (S. Kowalski, 1994), and other information security models, standards and best practices.

Security culture has been an important topic in the practitioner literature, and recently has been identified as an opportunity for future information security research (M. A. Alnatheer, 2015).

Based on the comprehensive review of the literature, the framework development consolidated using the socio-technical factors influencing information security. The two dimensions of candidate factors which set the influence on information security effectiveness based on the literature review analysis are:

- **Socio-technical dimension: which includes** (Legal & law, Compliance, Ethical Conduct, Security culture, Security Policy, Security Awareness, Security Training, Top Management Support)

- **Technical dimension: which include** (IS structure)

Furthermore, as discussed earlier, cultural factors might influence the effectiveness of security management practices and more particularly security culture.

In addition, existing research has shown that information security policies have positive influence on security effectiveness (S. M. Alfawaz, 2011; Chang & Lin, 2007; Kankanhalli et al., 2003). Security culture has been found as important factor which has a significant impact on information security effectiveness (Knapp & Ferrante, 2014). Other researches indicates that top management support, training, awareness influences security culture for information security positively effectiveness, (M. A. Alnatheer, 2014; Knapp et al., 2007). Organizational factors are said to shape the implementation of effectiveness information security management (Chang & Ho, 2006; Knapp et al., 2009). Management support and security culture also have a positive impact on security effectiveness (Brady, 2011; Knapp et al., 2007). The extent to which information systems are structured has an influence on information security effectiveness (Hussein et al., 2007). Information system structure has a direct impact on the effectiveness of information security (S. M. Alfawaz, 2011). Researchers have indicated that compliance is a crucial factor for information security effectiveness (Al-Tameem et al., 2009). Eloff and Eloff (2005) stated that security culture of the organization will improve by the information security compliance with the security policy. There is strong relationship between security compliance and security culture (D'Arcy & Greene, 2009). Eloff and Eloff (2005) argued that it is necessary to identify human elements such as policies, guidelines, standards, codes of practice, human issues, technology, ethical and legal issues which affect the effectiveness of the whole system in order to design strategies that can minimize their weakness. Security legal and ethics factors are important for addressing security problems. If such a framework is lacking, prosecuting people who commit illegal actions will not be effective (Chaula, 2006). Chang and Lin (2007) indicated that management support and security culture had a positive impact on effectiveness of information security. Further, Chang and

Lin stated that effectiveness was significantly correlated to basic security principles such as confidentiality, integrity, and availability.

Based on the results of the data analysis in chapter 4, with regard to the assessment of scale reliability, EFA and CFA of the survey data, the assessment of the scale reliability showed that the measurement scales, which were used to capture the meaning of the framework constructs, were reliable, as indicated by the high values of Cronbach's alpha for each individual construct. The item-total correlations of all the variables were also substantial, indicating that each variable adequately measured its underlying construct. However, reliability is only necessary, not a sufficient, condition for validity. As a result, factor analysis, including EFA and CFA, were performed to inform an evaluation of scale validity. EFA was conducted for each individual construct to uncover the appropriate number of latent factors (factor structures). The extracted factors from EFA were examined by the stricter CFA technique to confirm validity. For each construct, the results of the CFA provided the final factor structures that demonstrated adequate reliability and validity. In conclusion, it was confirmed that good measurement scales for the constructs were with very good reliability, validity and conceptual definitions. The results from the literature review, EFA and CFA sequentially were used to develop the framework. In addition, many studies have concluded that the information security culture is important factor that influence information security effectiveness (S. M. Alfawaz, 2011; M. A. Alnatheer, 2014; Adele Da Veiga & Nico Martins, 2015; Knapp & Ferrante, 2014). To manage security effectively, there is need to create security culture. Therefore security culture is defined as mediation factor between all of socio-technical factors and security effectiveness. Based on the comprehensive review of the literature in Figure 2.3, presents the framework Figure 5.1.

Based on the information security culture framework for securing e-government the main hypothesis to be tested through the subsequent survey phase are summarized in Table 3.1 (refer to chapter 3)

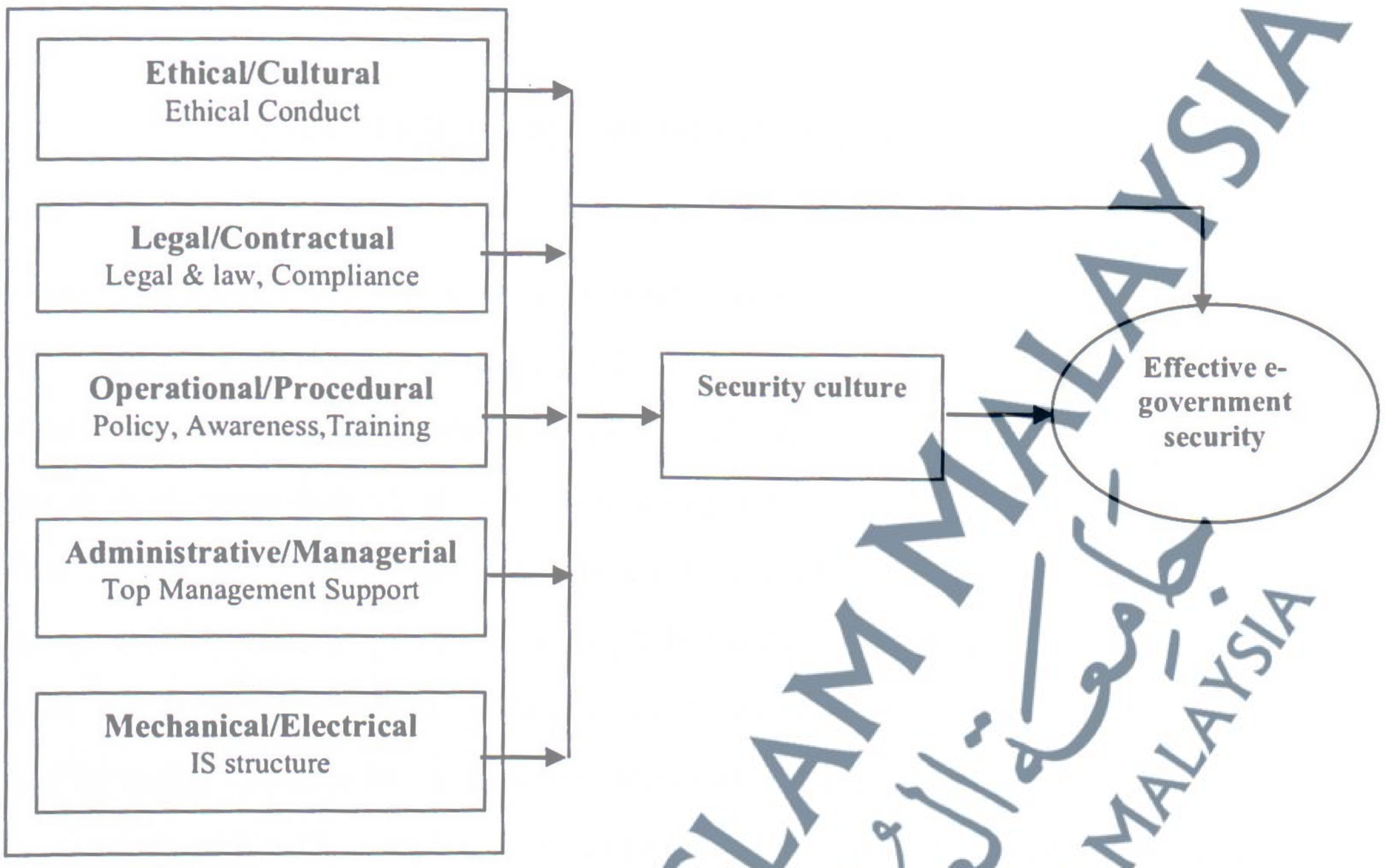

Figure 5.1: Information Security Culture Framework For Securing E-Government

5.3 Chapter Summary

This chapter presented the development steps of the proposed framework based on a comprehensive literature review and data analysis results. As the study aimed to validate this framework in subsequent stages of the research process with a survey questionnaire, the results form the basis for creating the factors that were used in the subsequent framework assessment, which is presented in the structure equation modeling next chapter 6.